AUDITORIA INFORMÁTICA

Germán E. Chávez S.

Manual Para Estudiantes

AUDITORIA INFORMÁTICA
MANUAL PARA ESTUDIANTES

Germán E. Chávez S.

MMXIV

Germán E. Chávez S.

Auditoría Informática Manual Para Estudiantes.

1ra edición - Barinas: 2014.

224 p.; 21,50 x 27,94 cms.

ISBN

www.germanchavez.com

¡Copie este libro!

"Una inversión en conocimiento siempre paga el mejor interés".

Benjamin Franklin

CONTENIDO

INTRODUCCIÓN

Actualmente los diferentes avances tecnológicos e informáticos, facilitan a las organizaciones la automatización de gran parte de sus procesos. De estos procesos se generan distintos volúmenes de información, los cuales tienen distintos niveles de importancia o valor para las organizaciones. Al ver la información como un activo de la organización, es necesario idear mecanismos para proteger esos activos.

La auditoría informática se encuentra en auge debido a que los nuevos paradigmas tecnológicos hacen necesaria la evaluación de los controles informáticos en las organizaciones, con la finalidad de medir los niveles de protección de los activos de información.

La idea de realizar este "manual para estudiantes" se centra en plantear una guía detallada para que los lectores puedan iniciar en el mundo de la auditoría informática. Cabe destacar que este texto busca esbozar una metodología de trabajo sencilla y clara, donde se detallan algunos de los conceptos, técnicas e instrumentos más utilizados y algunas recomendaciones para su construcción e implementación.

El objetivo fundamental de este texto consiste en orientar a estudiantes de pregrado que desean realizar una auditoría informática como trabajo especial de grado, brindando las herramientas necesarias para incursionar en esta área. Sin embargo, las fases, técnicas e instrumentos que se especificarán a lo largo del manual, pueden ser fácilmente adaptadas para otros tipos de auditorías. Es importante destacar, que este manual no se limita exclusivamente para el uso de estudiantes, también puede ser de gran a profesionales que requieren conocimientos en este campo de la informática.

El presente manual está conformado por cinco capítulos, donde los dos primeros consisten en conceptos relacionados con la auditoría y seguridad informática, para luego, plantear mediante los tres últimos capítulos, la estructura necesaria para realizar una auditoría informática.

Dado el público al cual está dirigido este trabajo, se asume que el lector, posee un nivel de conocimientos informáticos adecuado para la compresión de este libro, sin embargo, a lo largo de los distintos contenidos, se trata de explicar todos los conceptos e ideas de la forma más sencilla posible y adicionalmente se incluye un glosario de términos relacionados con la auditoría informática y la informática en general.

Finalmente, es sumamente importante destacar, que la mayoría de los formatos e instrumentos recopilados en este manual, han sido diseñados tras un largo trabajo de investigación por la **Dra. Mailen Camacaro R.** quien ha sido parte fundamental en de la formación del autor en materia de control, auditoría y gestión.

CAPÍTULO I

FUNDAMENTOS DE AUDITORÍA

Antes de mostrar el concepto formal de auditoría, es importante conocer dos conceptos muy importantes en esta área de estudios y que a veces suelen confundirse entre sí, estos son: eficiencia y eficacia. En palabras simples, la **eficacia** consiste en cumplir los objetivos o resultados planteados, sin importar los medios empleados y la **eficiencia** consiste en optimizar los recursos, sin embargo, esto no implica necesariamente que se logren los resultados esperados.

El Chapulín colorado es un ejemplo de un individuo eficaz, logra siempre el resultado, incluso sin darse cuenta, valiéndose de cualquier medio.

Willy Coyote es un claro ejemplo de un individuo eficiente, optimiza los recursos para construir las trampas, sin embargo, nunca puede comerse al correcaminos.

Figura 1. Diferencias entre eficacia y eficiencia.

Se puede decir ahora, que al lograr eficacia y eficiencia, se obtiene la **efectividad**. Se optimizan los recursos empleados y se logran los resultados planteados.

Ahora, ya tenemos los recursos necesarios para definir el concepto de auditoría. La auditoría es un **Examen Crítico**, que se realiza con objeto de evaluar la eficiencia y la eficacia de una sección o de un organismo, y determinar cursos alternativos de acción para mejorar la organización, y lograr los objetivos propuestos.

En una sola palabra, se puede resumir el concepto de auditoría como una **EVALUACIÓN**. Esta evaluación pretende medir la efectividad del área auditada.

La auditoría que normalmente conocemos, es la financiera, se trata de un proceso, cuyo resultado final es realizar la emisión de un informe en el cual, el auditor revela su opinión acerca de la situación financiera de una empresa; este proceso solo puede llevarse a cabo mediante un elemento denominado Evidencia de Auditoría, debido a que el auditor realiza su trabajo posteriormente a las operaciones de la empresa. Es muy común que las organizaciones realicen este tipo de auditorías cuando sospechan sobre fallas en las cuentas o simplemente para conocer el estado de la organización.

AUDITORÍA INTERNA Y EXTERNA

Existen diferentes áreas que se pueden auditar (auditoría financiera, auditoría informática, auditoría de procesos de producción, entre otras), sin embargo existen básicamente solo dos tipos de auditoria: Auditoria Interna y Auditoría Externa. La diferencia principal entre estos dos tipos de auditoría radica en el personal que las realiza, es decir, la auditoría interna es realizada por personal que labora en la organización, usualmente existe en las organizaciones grandes, algún departamento de contraloría que cuenta con personal capacitado que se especializa en este tipo de evaluaciones. La auditoría externa, por otra parte, es realizada por

profesionales que no forman parte de la organización y que son contratadas por la misma para evaluar desde otro ángulo, el desempeño del área en cuestión.

Ambos tipos de auditoría tienen sus ventajas y desventajas, por una parte, la auditoría interna tiene como ventaja que el personal conoce bien (o debería ser así) los procesos de la organización, por lo que podría resultar más fácil la aplicación de pruebas y recolección de evidencias. Una posible desventaja de este tipo de auditoría consiste en que al pertenecer a la organización, el auditor se vea limitado a no señalar algunas fallas o inconsistencias para “no afectar” a algunos compañeros de trabajo responsables de las áreas auditadas.

Por otra parte, la principal ventaja que tiene la auditoría externa, es que el auditor no tiene vínculos con la organización, por lo cual se espera que sea más objetivo y profesional, pero se encuentra con la posible desventaja de ser visto como un extraño que va a la organización a realizar una cacería de brujas y el personal del área auditada podría poner trabas o resistencia al momento de brindar la información necesaria para al proceso de auditoría.

Este manual está orientado hacia la realización de una auditoria externa, aun cuando el estudiante pudiese formar parte de la organización que utiliza como objeto para su investigación. El alumno podría argumentar que entre las técnicas de recolección de datos que utiliza para su trabajo se encuentra la observación directa ya que el investigador forma parte de la organización, sin embargo, para el proceso de auditoría se recomienda que el estudiante se vea así mismo como una persona externa y de esta manera evita omitir algunas pruebas.

AUDITORÍA INFORMÁTICA

Luego de haber definido diversos conceptos a lo largo de este capítulo, ya estamos en capacidad para dar una definición formal de la auditoría informática. La auditoría informática es un proceso llevado a cabo por **profesionales especialmente capacitados para el efecto**, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

Las auditorías informáticas permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costos, valor y barreras, que obstaculizan flujos de información eficientes.

Los principales objetivos que constituyen a la auditoría informática son el control de la función informática, el análisis de la eficiencia de los Sistemas Informáticos, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales, humanos e informáticos.

Si recordamos un poco sobre teoría de sistemas, podemos definir un sistema (de cualquier tipo) como un conjunto de partes que funcionan en conjunto para lograr un fin específico, por lo cual es pertinente aclarar, que al hablar de sistemas, no utilizamos exclusivamente el término para los programas o software, sino que puede ser utilizado para referirnos a procesos o procedimientos que forman parte del entorno informático de la organización. Por tanto, una auditoría de sistemas no se limita solamente a

los programas o dispositivos, sino que puede incluir en su alcance, la evaluación de procedimientos o normativas relacionadas con los aspectos tecnológicos o de flujo de información de la organización.

Al lector le puede parecer contradictorio el hecho de que en la definición de auditoría informática se incluye la frase: “profesionales especialmente capacitados para el efecto”, y que este texto tenga como objetivo convertirse en un “manual para estudiantes” o principiantes en el área de la auditoría. Lo ideal es que las personas que se dedican a evaluar, tengan gran dominio de las áreas que van a evaluar y de las herramientas y estrategias que utilizarán para evaluar. Sin embargo, un estudiante que finaliza una carrera de ingeniería o licenciatura en informática, sistemas, computación u otra similar, debe manejar los conceptos fundamentales de las distintas áreas que conforman el entorno informático de una organización, tales como: bases de datos, procesos de desarrollo, redes, seguridad, sistemas operativos, entre otras. Por lo tanto, para poder lograr los objetivos al plantear una auditoría como trabajo final de grado (tesis), sólo hace falta orientación sobre el proceso de auditoría en sí mismo, el cual será desarrollado a lo largo de los distintos capítulos que conforman este instructivo.

En Venezuela, para poder realizar auditorías de cualquier tipo a entidades públicas, es necesario cumplir un proceso, mediante el cual la Contraloría General de la República, acredita a los auditores (Registro de Auditores, Consultores y Profesionales Independientes) y una vez avalados por esta acreditación, pueden postularse para los distintos procedimientos de auditorías. Debido a esta limitante, es necesario que el estudiante tenga en cuenta esta información a la hora de proponer una auditoría informática en algún ente del estado.

TIPOS DE AUDITORÍA INFORMÁTICA

En una determinada organización, pueden encontrarse distintos recursos informáticos que pueden ser evaluados, diferentes aspectos a evaluar de cada uno de estos recursos y diversas maneras de evaluar cada uno de dichos aspectos.

Figura 3. Aspectos a evaluar mediante la auditoría informática.

Existen diversos tipos de auditoría informática, tales como:

- Auditoría de la gestión.
- Auditoría legal (Ley Orgánicas de Protección de datos y firmas electrónicas).
- Auditoría de los datos (Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas).
- Auditoría de las bases de datos.
- Auditoría de la seguridad (física y/o lógica).
- Auditoría de las comunicaciones.
- Auditoría de la seguridad en producción (Frente a errores, accidentes y fraudes).
- Auditoría informática de sistemas.
- Auditoría informática de explotación.
- Auditoría informática de desarrollo.

AUDITORÍA INFORMÁTICA FORENSE

Los sistemas de información adquieren un papel cada vez más relevante en nuestra actividad diaria. Los robos de información, fraude, manipulación y abusos de los correos electrónicos, ataques a web, accesos no autorizados, etc, son algunas de las muestras de los peligros que acechan a la empresa. Esto ha obligado a la obtención y evaluación de pruebas de los sistemas. Estas pruebas con un alto nivel técnico hacen necesaria, en muchos casos, una interpretación por parte de peritos o especialistas que realicen una auditoria de peritaje y auditoría forense. En la mayoría de los casos, la auditoría forense se encuentra estrechamente relacionada con investigaciones judiciales (pornografía infantil, estafas, entre otros), donde la obtención de evidencias digitales funciona como pruebas, sin embargo, muchas organizaciones implementan esta modalidad de auditoría cuando sospechan que han sido vulnerados sus sistemas.

El lector debe estar familiarizado con el hecho de que toda actividad que realizamos en el computador o en Internet, deja algún rastro o registro que puede ser seguido a menos que se tomen las medidas necesarias para cubrirlos.

Figura 4. Auditoría Forense.

Debido a las técnicas avanzadas que se utilizan para este tipo de auditoría, en las que se puede destruir o corromper la evidencia al no ser manipulada apropiadamente, no será contemplada dentro de los objetivos de este texto. Se hará énfasis en cinco tipos de auditoría informática (sistemas, bases de datos, procesos de desarrollo de software, seguridad y redes), para los cuales se dedicará un capítulo a cada una de las mismas. Invitamos al lector a indagar un poco más sobre los otros tipos de auditoría informática y sus procedimientos.

IMPORTANCIA DE LA AUDITORÍA INFORMÁTICA

La importancia de realizar periódicamente auditorías informáticas en las organizaciones, radica en que mediante éstas, se puede ir mejorando el ecosistema informático de la organización. La auditoría informática permite evaluar el estado de los activos informáticos con la finalidad de detectar posibles fallas o errores y de esta forma proponer soluciones factibles que puedan ser tomadas en consideración por la organización. Es necesario resaltar que el papel del auditor no consiste en solucionar los problemas antes mencionados, sino, brindar a la empresa un informe donde se señalan estos problemas y así, sea la misma organización la que se encargue en tomar las medidas necesarias para resolverlos y evitar sus causas.

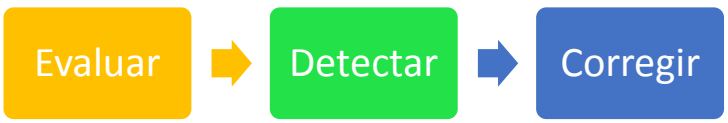


Figura 5. Importancia de la auditoría informática.

FASES DE LA AUDITORÍA INFORMÁTICA

No existe una forma única de realizar la auditoría informática, los procedimientos pueden variar dependiendo del auditor o grupo de auditores, existen algunas metodologías para realizar auditorías (ejemplo: OSSTMM para auditoría de redes), sin embargo, hay un compendio de estándares llamadas **Normas de Auditoría Generalmente Aceptadas** (NAGAS), que proponen realizar la auditoría básicamente en 3 fases y mediante las cuales se desarrolla este instructivo.

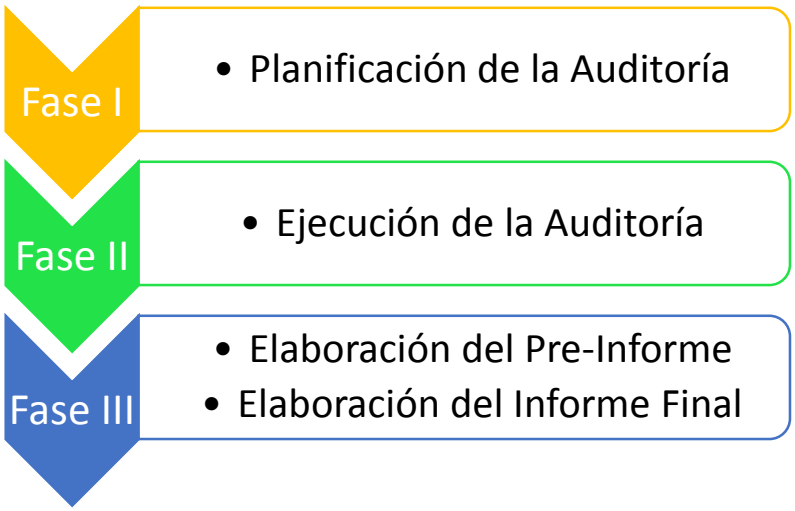


Figura 6. Fases de la auditoría informática.

La Norma de Auditoría Generalmente Aceptadas (NAGAS) son los principios fundamentales de auditoría a los que deben enmarcarse su desempeño los auditores durante el proceso de la auditoria. El cumplimiento de estas normas garantiza la calidad del trabajo profesional del auditor.

Las Normas de Auditoría Generalmente Aceptadas están constituidas por un grupo de 10 normas adoptadas por el American Institute Of Certified Public Accountants y que obliga a sus miembros, su finalidad es garantizar la calidad de los auditores.

Las normas tienen que ver con la calidad de la auditoría realizada por el auditor independiente. Los socios del AICPA han aprobado y adoptado diez normas de auditoría generalmente aceptadas (NAGA), que se dividen en tres grupos:

En la actualidad las NAGAS, vigentes son 10, las mismas que constituyen los (10) diez mandamientos para el auditor y son:

Normas Generales o Personales

1. Entrenamiento y capacidad profesional
2. Independencia
3. Cuidado o esmero profesional.

Normas de Ejecución del Trabajo

4. Planeamiento y Supervisión
5. Estudio y Evaluación del Control Interno
6. Evidencia Suficiente y Competente

Normas de Preparación del Informe

7. Aplicación de los Principios de Contabilidad Generalmente Aceptados.
8. Consistencia
9. Revelación Suficiente
10. Opinión del Auditor

CAPÍTULO II

SEGURIDAD Y CONTROL

Seguridad de información es mucho más que establecer “firewalls”, aplicar parches para corregir nuevas vulnerabilidades en el sistema de software, o guardar en la bóveda los “backups”. Seguridad de información es determinar qué requiere ser protegido y por qué, de qué debe ser protegido y cómo protegerlo.

La información es un activo, que tal como otros importantes activos del negocio, tiene valor para una empresa y consecuentemente requiere ser protegida adecuadamente. Cualquier forma que tome la información (digital, impresa, entre otras), o los medios que se utilicen para compartirla o almacenarla, siempre debe estar apropiadamente protegida.

La seguridad de información se caracteriza por la preservación de:

Confidencialidad: La información está protegida de personas no autorizadas.

Integridad: La información está como se pretende, sin modificaciones inapropiadas.

Disponibilidad: Los usuarios tienen acceso a la información y a los activos asociados cuando lo requieran.

Se puede definir **Riesgo**, como “la combinación de la probabilidad de un evento y sus consecuencias”. Para efectos de nuestro estudio, los riesgos

son eventos que pueden afectar la seguridad de nuestros activos, ya sean a nivel de hardware, software o simplemente a nivel de información.

Una **Amenaza** consiste en una declaración del intento de hacer daño, su principal característica es que tienen potencial para causar un incidente no deseado. Podemos encontrarnos con 4 tipos de amenazas:

- Desastres naturales (inundaciones, terremotos, huracanes, etc.).
- Humanos (falta de personal, error de mantenimiento, error de usuario).
- Tecnológico (fallas en la red, tráfico sobrecargado, fallas de hardware).
- Amenazas deliberadas

Dentro de la última categoría resaltan dos términos con los que el lector posiblemente esté familiarizado, el primero de ellos es la palabra **Hacker**, y se refiere a personas que tienen cierto nivel de conocimientos para violentar sistemas informáticos y obtener cierta información privilegiada con la finalidad de satisfacer su ego o de lucrarse económicamente. El segundo término que podemos mencionar al hablar de amenazas, es la **Ingeniería Social**, un término popularizado por Kevin Mitnick, un hacker reconvertido en consultor (Hacker Ético), “es el acto de engañar a la gente para que haga algo que no desea o para que proporcione información confidencial”.

Figura 7. Hackers e Ingeniería Social.

Por otra parte, una **Vulnerabilidad** es una debilidad en el sistema de seguridad de información. Una vulnerabilidad puede hacer que una amenaza se materialice al ser aprovechada, sin embargo una vulnerabilidad no causa daño, es simplemente una condición o conjunto de condiciones que pueden hacer que una amenaza afecte a un activo.

Algunas posibles vulnerabilidades son:

- Ausencia de personal clave.
- Falta de entrenamiento en seguridad.
- Líneas de cableado desprotegidas.
- Puertas sin cerraduras.
- Ausencia de antivirus.
- Ausencia de conciencia de seguridad.
- Política no clara de contraseñas.

Figura 8. Ejemplo de vulnerabilidad.

Para los fines de la auditoría informática, las amenazas y vulnerabilidades tienen el mismo nivel de importancia, ya que pueden afectar las actividades de la organización. Es necesario detectarlas para poder recomendar las medidas necesarias para su solución.

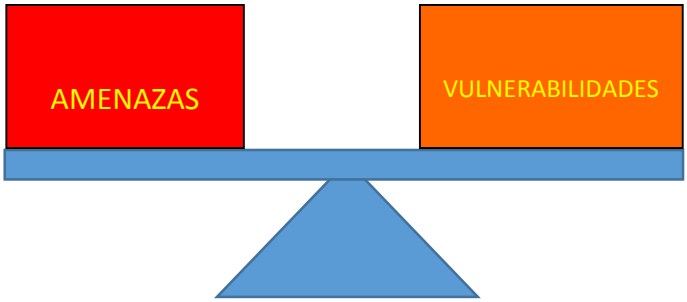


Figura 9. Amenazas y Vulnerabilidades.

Existen tres fuentes para que una organización identifique sus requerimientos de seguridad:

La primera fuente deriva de la evaluación de los riesgos que afectan la organización. Aquí se determinan las amenazas de los activos, luego se ubican las vulnerabilidades y se evalúa su posibilidad de ocurrencia, y se estiman los potenciales impactos.

La segunda fuente es el aspecto legal. Aquí están los requerimientos contractuales que deben cumplirse.

La tercera fuente es el conjunto particular de principios, objetivos y requerimientos para procesar información, que la empresa ha desarrollado para apoyar sus operaciones.

La seguridad de la información protege la información de una serie de amenazas para que así la empresa pueda continuar operando, minimizar daños a la gestión comercial y maximizar el retorno a la inversión y oportunidades de negocios.

Cada organización tendrá un conjunto de requerimientos diferentes de control y de niveles de confidencialidad, integridad y disponibilidad.

ANÁLISIS DE RIESGOS

La alta dependencia de los sistemas de información trae cada vez más, preocupación en las organizaciones debido a los riesgos que generan la complejidad de los sistemas, posibles accidentes, errores o ataques, y la constante evolución en un entorno cambiante; por lo que la ejecución de estos riesgos puede afectar la continuidad de los servicios (internos y externos), la protección de la información en general, así como la validez y eficacia de los procesos que se basan en transacciones electrónicas; por lo tanto, es necesario aplicar un análisis de riesgos para crear las políticas de seguridad basadas en una metodología para controlar los elementos que permiten reducir la exposición a los riesgos protegiendo los activos de una organización.

Es fundamental aclarar que los riesgos no se pueden eliminar por más medidas que se tomen, pero si se pueden mitigar, de tal manera que el análisis de riesgos nos permite conocer los posibles riesgos de la organización y a su vez proponer medidas para minimizarla ocurrencia o el impacto de estos riesgos, para de este forma asegurar los activos.

La evaluación de riesgos es una técnica usada para examinar unidades auditables dentro del universo de auditoría informática y para seleccionar áreas a revisar que tengan la mayor exposición a riesgos. Una unidad auditable se define como un segmento discreto de la organización, junto con sus sistemas. La determinación del universo de auditoría debe basarse en el conocimiento del plan estratégico de TI de la organización, en sus operaciones y en discusiones con la gerencia a cargo.

Deben efectuarse ejercicios de evaluación de riesgos para facilitar el desarrollo del plan de auditoría, los cuales deben documentarse al menos anualmente. Los planes estratégicos de la organización, los objetivos y el

marco de administración de riesgos de la empresa deben considerarse como parte del ejercicio de evaluación de riesgos.

El uso de la evaluación de riesgos en la selección de proyectos de auditoría permite al auditor cuantificar y justificar los recursos de auditoría necesarios para completar el plan de auditoría de SI o una revisión en particular. Asimismo, el auditor puede priorizar las revisiones programadas basándose en la percepción de riesgos y contribuir a la documentación de marcos de administración de riesgos.

Un auditor debe realizar una evaluación preliminar de los riesgos relevantes al área bajo revisión. Los objetivos del contrato de auditoría deben reflejar los resultados de dicha evaluación de riesgos.

Después de terminar la revisión, el auditor debe asegurarse de que se actualice la estructura de administración/gestión de riesgos empresariales de la organización o su registro de riesgos, en caso de haberse desarrollado alguno, a fin de reflejar los hallazgos y recomendaciones de la revisión así como la actividad subsiguiente.

OBJETIVOS DEL ANÁLISIS DE RIESGOS

El proceso de análisis de riesgo deber ser efectuado en cualquier momento y cumplir con los siguientes objetivos: Identificar, evaluar, y manejar los riesgos de seguridad; debe estimar la exposición de un recurso a una amenaza específica; determinar cuál combinación de medidas de seguridad proporcionará un nivel de seguridad razonable a un costo aceptable; tomar mejores decisiones en seguridad informática y enfocar recursos y esfuerzos en la protección de los activos de información.

BENEFICIOS DEL ANÁLISIS DE RIESGOS

El realizar un análisis de riesgos en las organizaciones trae consigo una serie de beneficios que se ven reflejados en el costo-beneficio de la misma, éstos varían de organización en organización y van de acuerdo a las políticas de cada una, pero en líneas generales se resumen de la siguiente manera:

- Asegurar la continuidad operacional de la empresa
- Saber manejar las amenazas y riesgos críticos
- Mantener una estrategia de protección y de reducción de riesgos
- Justificar una mejora continua de la seguridad informática.
- Costos de seguridad justificados
- Permitir que la seguridad se convierta en parte de la cultura de la organización
- Apoyar la comunicación y facilitar la toma de decisiones, certeza económica/financiera.

LIMITANTES DEL ANÁLISIS DE RIESGOS

El proceso de análisis de riesgos presenta una serie de limitantes como son: complicaciones para concienciar objetivos, ligereza en la aplicación de los análisis en el campo, escasa difusión, poca concienciación, gran diversidad de métodos de análisis, inversión de tiempo y recursos a las actividades, las soluciones al problema de seguridad no son instantáneas, y una sola metodología no es aplicable a todos los ambientes.

FASES DEL ANÁLISIS DE RIESGOS

El proceso de análisis de riesgos debe cumplir con tres etapas:

Fase 1: construir perfiles de amenazas basados en activos: activos críticos, requerimientos de seguridad para los activos críticos, amenazas a los activos críticos, prácticas de seguridad actuales, vulnerabilidades actuales de la organización.

Fase 2: identificar vulnerabilidades de infraestructura: componentes clave, vulnerabilidades actuales de la tecnología.

Fase 3: desarrollar planes y estrategias de seguridad: riesgos de los activos críticos, medidas de riesgo, estrategias de protección, planes de mitigación de riesgos.

Como se ha mencionado anteriormente, los riesgos no pueden eliminarse completamente, solo mitigarse. Existen varias maneras en las que la organización puede tratar el riesgo, en todo caso, dependerá de la gerencia correspondiente.

- La primera forma de tratar el riesgo consiste en la **Reducción del Riesgo** y consiste en tomar las medidas adecuadas para que disminuir el impacto o la ocurrencia de los riesgos. Para todos aquellos riesgos donde la opción de reducir el riesgo ha sido escogida, se debieran implantar controles apropiados para reducir los riesgos al nivel que ha sido identificado como aceptable, o por lo menos lo más cercano posible.
- La segunda forma es la **Aceptación del Riesgo** y se basa en lo que la organización considera “aceptable” para continuar con sus operaciones normales. Es posible que existan algunos riesgos para los cuales la organización no puede identificar controles o el costo del control sobrepasa la potencial perdida si ocurriese el riesgo. En estos casos se puede tomar la decisión de aceptar el riesgo y vivir con las consecuencias, si ocurriera. Un posible ejemplo de esta

aceptación, es la pérdida de información durante un proceso de respaldo de archivos, en este caso, la organización debe definir previamente que porcentaje de pérdida de esta información es permitida.

- La tercera manera consiste en **Transferir el Riesgo.** La transferencia del riesgo es una opción cuando es difícil para una compañía reducir o controlar el riesgo a un nivel aceptable. Un claro ejemplo podría ser la contratación de una empresa especializada (outsourcing) para configurar una antena y así evitar que las comunicaciones sean interceptadas.
- Por último se puede **Evitar el Riesgo** y sencillamente se trata de describir acciones donde, actividades del negocio o maneras de realizarlas son modificadas para evitar la ocurrencia del riesgo. Algunas formas de evitar el riesgo podrían ser: No conducir ciertas actividades, Mover los activos de una zona considerada riesgosa, Decidir no procesar información particularmente sensitiva.

Es posible que la organización use algunas e incluso todas las formas anteriores de tratar el riesgo, sin embargo como los riesgos no pueden ser eliminados, siempre quedará el llamado **Riesgo Residual**.

Debe evaluarse cuánto las decisiones ayudan a reducir el riesgo y cuánto queda del riesgo residual. El riesgo residual puede ser difícil de evaluar, pero por lo menos un estimado debe ser hecho para asegurar que se tiene instaurada la suficiente protección.

CONTROLES Y ESTÁNDARES

El control es una etapa primordial en la administración (de cualquier área de la organización), pues, aunque una empresa cuente con magníficos planes, una estructura organizacional adecuada y una dirección eficiente,

el ejecutivo no podrá verificar cuál es la situación real de la organización si no existe un mecanismo que se cerciore e informe si los hechos van de acuerdo con los objetivos.

Se puede definir **Control**, como el proceso de medir los actuales resultados en relación con los planes, diagnosticando la razón de las desviaciones y tomando las medidas correctivas necesarias.

También hay otras connotaciones para la palabra control:

- Comprobar o verificar;
- Regular;
- Comparar con un patrón;
- Ejercer autoridad sobre alguien (dirigir o mandar);
- Frenar o impedir.

En la auditoría informática, los controles pueden reducir el riesgo valorado en muchas maneras:

- Reduciendo la posibilidad de que la vulnerabilidad sea explotada por la amenaza.
- Reduciendo el posible impacto si ocurriera el riesgo, detectando eventos no deseables, reaccionando y recuperándose de ellos.

Un concepto estrechamente relacionado con el control es el **Gobierno de TI**, el cual consiste en liderar, concebir y gerenciar procesos y estructuras que aseguren que la TI esté alineada con la estrategia del Negocio, que contribuye al logro de los objetivos, controla los riesgos y asegura que los recursos son utilizados responsable y apropiadamente.

ISACA Y COBIT

ISACA (Information Systems Audit and Control Association) es una organización internacional dedicada a promover y expandir los conocimientos y el valor en el campo del gobierno y control de TI. Inició sus actividades en 1969, abarca 160 países, dividida en 175 capítulos y cuenta con alrededor de 86.000 asociados. Mantienen las publicaciones: Information Systems Control Journal y Acredita a los auditores mediante las Certificaciones: CISA, CISM, CGIT y CRISC.

ISACA ha elaborado un marco de gobierno de las tecnologías de información llamado **COBIT** (actualmente en su versión 5), que proporciona una serie de herramientas para que la gerencia pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio. De esta manera, COBIT funciona como una guía de buenas prácticas para el gobierno de la TI en las organizaciones. Entre las principales características de COBIT destacan:

- Permite el desarrollo de las políticas y buenas prácticas para el control de las tecnologías en toda la organización.
- Enfatiza el cumplimiento regulatorio, ayuda a las organizaciones a incrementar su valor a través de las tecnologías, y permite su alineamiento con los objetivos del negocio.
- Ayuda a las Organizaciones a crear un valor óptimo a partir de la TI, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos.
- COBIT 5 permite que las tecnologías de la información y relacionadas se gobiernen y administren de una manera holística a nivel de toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios,

considerando los intereses relacionados con la TI de las partes interesadas internas y externas.

- Los **principios** y **habilitadores** de COBIT 5 son genéricos y útiles para las Organizaciones de cualquier tamaño, bien sean comerciales, sin fines de lucro o en el sector público.

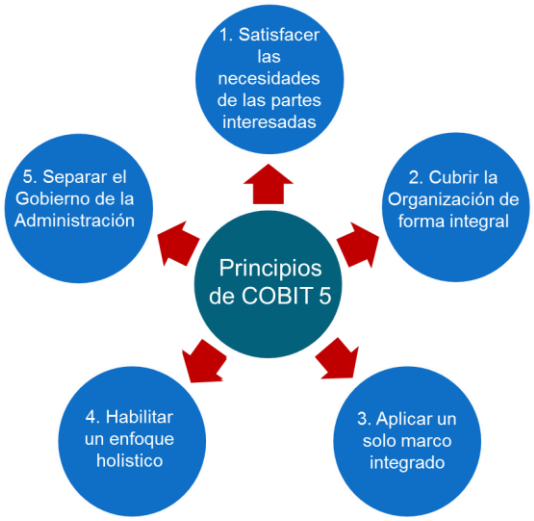


Figura 10. Principios de COBIT 5. Fuente: COBIT® 5, © 2012 ISACA® Todos los derechos reservados.

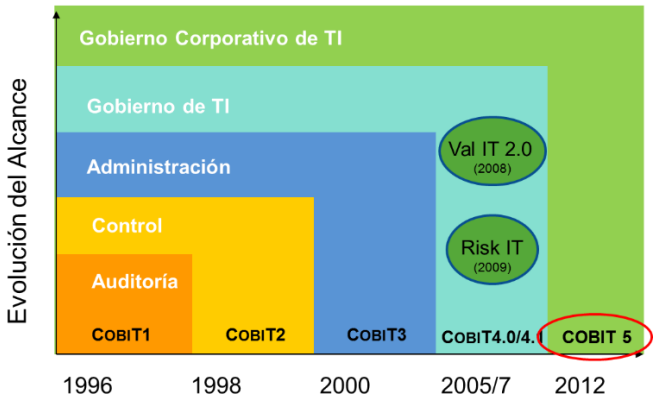


Figura 11. Evolución del alcance de COBIT. Fuente: COBIT® 5, © 2012 ISACA® Todos los derechos reservados.

ISO/IEC FAMILIA 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Dentro de esta familia de estándares encontramos algunas normativas que rigen el análisis de riesgos:

ISO/IEC 27001:2005 (Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos). Aprobado y publicado como estándar internacional en Octubre del 2005 por Específica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de seguridad de información (SGSI).

ISO/IEC 27005:2008 Norma que proporciona directrices para la gestión del riesgo de seguridad de la información en una organización, sin embargo, esta norma no proporciona ninguna metodología específica para el análisis y la gestión del riesgo de la seguridad de la información.

ISO/IEC 27002:2005 (Antigua ISO/IEC 17799): Tecnología de la información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

En el capítulo IV (Ejecución de la Auditoría) aprenderemos a utilizar los estándares (controles) para realizar la auditoría informática, en particular, emplearemos algunas de las normas ISO/IEC antes mencionadas.

NOTAS DEL LECTOR

El lector puede aprovechar este espacio para escribir algunas notas relacionadas con los tópicos estudiados en los primeros capítulos.

CAPÍTULO III

FASE I: PLANIFICACIÓN DE LA AUDITORÍA

La primera fase de la auditoría corresponde a la etapa preliminar, aquí se describen los pasos a seguir durante el resto de la auditoría, por lo cual es quizás la parte más compleja de todas. Aunque el proceso de auditoría puede ser un poco flexible y de ser necesario permite incorporar nuevos procedimientos posteriormente, es altamente recomendable tomarse el tiempo debido para planificar y realizar una **Estimación de Recursos y Tiempos** lo más real posible. El proceso de planificación se realiza en un orden secuencial, donde cada una de las tareas será realizada en base a la información generada en la tarea que le precede, de allí proviene la importancia de relacionar correctamente todos los elementos de la auditoría para alinearlos estratégicamente y garantizar el éxito del auditor.

La planeación del trabajo tiene como significado, decidir con anticipación todos y cada uno de los pasos a seguir para realizar el examen de auditoría. Para cumplir con esta norma, el auditor debe conocer a fondo la Empresa que va a ser objeto de su investigación, para así planear el trabajo a realizar, determinar el número de personas necesarias para desarrollar el trabajo, decidir los procedimientos y técnicas a aplicar así como la extensión de las pruebas a realizar. La planificación del trabajo incluye aspectos tales como el conocimiento del cliente, su negocio, instalaciones físicas, colaboración del mismo etc.

Por otra parte, a pesar de que este es una guía para estudiantes o “novatos de la auditoría”, es importante comentar que en esta etapa se establecen las horas estimadas para la realización del trabajo, los

honorarios correspondientes a estas horas de trabajo, las condiciones de pago y el periodo de contratación.

Cabe destacar que si nos dedicamos a la auditoría para ganarnos la vida, no podemos darnos el “lujo” de perder tiempo innecesariamente por no haber planificado bien en primera instancia, o en el peor de los casos, tener que comprar licencias de software o contratar personal de apoyo que no estaban contemplados inicialmente y perder dinero a causa de esto. El auditor debe ser profesional y apegarse al presupuesto que se le plantea al cliente, si la planificación está mal hecha es el auditor quien debe correr con las consecuencias.

En esta primera etapa se contemplan las siguientes actividades:

- Determinación del tiempo para realizar la auditoria.
- Determinar el equipo de trabajo a participar en el proyecto.
- Determinación de las herramientas informáticas a emplear en la auditoría.
- Determinar los recursos materiales necesarios para realizar la auditoría.

NRO	ACTIVIDAD	TIEMPO
1	Planificación de las actividades	10 Horas
2	Levantamiento inicial de información.	10 Horas
3	Definición de las técnicas e instrumentos de recolección de información.	20 Horas
4	Implementación de las técnicas e instrumentos de recolección de información.	60 Horas
5	Conclusiones	
6	Elaboración del Pre- Informe	12 Horas
7	Elaboración del informe final.	08 Horas

Cuadro 1. Ejemplo: Duración de las Tareas.

NRO	ACTIVIDAD	TIEMPO	RECURSOS
1	Planificación de las actividades	10 Horas	Lápiz, papel, PC, Impresora.
2	Levantamiento inicial de información.	10 Horas	Lápiz, Papel, Tablet.
3	Definición de las técnicas e instrumentos de recolección de información.	20 Horas	Lápiz, papel, PC, Impresora.
4	Implementación de las técnicas e instrumentos de recolección de información.	60 Horas	Lápiz, papel, Laptop, Software: NetTools, NetSupport Manager.
5	Conclusiones		Lápiz, papel, PC, impresora.
6	Elaboración del Pre- Informe	12 Horas	Lápiz, papel, PC, impresora.
7	Elaboración del informe final.	08 Horas	Lápiz, papel, PC, impresora.

Cuadro 2. Ejemplo: Estimación de los Recursos.

Usualmente el presupuesto va acompañado por una carta de presentación que puede ser similar al siguiente ejemplo:

Caracas, 19 de Agosto de 2014

Ciudadano
Licdo. Pedro Pérez
Director
Empresa XYZ
Su despacho.-

Reciba un cordial saludo, por medio de la presente le hago entrega del presupuesto estimado de consultoría, para la realización de la Auditoría Informática de….., para su análisis y consideración. Es oportuno mencionar que el alcance del trabajo presentado, comprende:

Fase I. Etapa Preliminar
Fase II. Desarrollo de la Auditoria
Fase III. Informe

Asimismo, para cualquier información adicional que requiera en relación a la propuesta planteada, favor comunicarse con mi persona a través del número telefónico: xxx-yyyyyyy

Atentamente

Ing. Pablo Gómez

Al momento que la organización aprueba el presupuesto, es recomendable realizar algún contrato o acta donde se especifiquen claramente los aspectos considerados anteriormente, además del alcance que tendrá la auditoría.

ALCANCE

El alcance identifica el **tipo** de auditoria informática a realizar, el tipo de software a auditar de ser el caso, la empresa a auditar y el tiempo. Al definir claramente el alcance, el auditor delimita el área a evaluar. Una auditoría informática puede ser tan amplia como se quiera, por lo cual, realizar bien esta actividad mantendrá al auditor encaminado en la dirección correcta.

TIEMPO ESTIMADO

Otra de las actividades importantes de la etapa de planificación de la auditoría informática es la de estimar correctamente el tiempo a utilizar. Se recomienda que el tiempo se exprese en horas y es necesario que se contemplen todas las actividades y tareas que serán realizadas durante todas las fases de la auditoría, incluyendo las horas utilizadas para elaborar el alcance, estimar el tiempo y redactar los objetivos. Por ejemplo, una auditoría promedio podría cubrir unas 120 horas o muchas más, dependiendo del alcance de la misma.

OBJETIVOS

La auditoría va orientada por algunos objetivos, los mismos se redactan de tal manera que manifiesten los propósitos o metas que el auditor espera alcanzar a través del proceso de auditoría informática. Como en la mayoría de las investigaciones o proyectos, los objetivos constan de un **Objetivo General** y algunos **Objetivos Específicos**.

El Objetivo General incluye el verbo de acción al alcance de la auditoria, por ejemplo: Realizar una Auditoria Informática de…

Los Objetivos Específicos describen las actividades principales que serán realizadas a lo largo de la auditoría. Para la redacción de los objetivos se recomienda al lector utilizar la Taxonomía de Bloom (ver anexo A), una tabla en la cual se plasman los verbos más comunes utilizados para tal fin. A modo de ejemplo se muestran a continuación cuatro expresiones que son bastante utilizados para redactar los objetivos específicos de una auditoría informática.

- Diagnosticar
- Evaluar el Control Interno Informático
- Analizar
- Presentar un Informe

MATRIZ DE ANÁLISIS DE AUDITORÍA

Una de las actividades más importantes de la fase de planificación consiste en la elaboración de la matriz de análisis de auditoría. Esta matriz es el corazón de la planificación, en ella ubican los objetivos (conceptos), se establecen las **Dimensiones**, que hacen referencia a los aspectos o facetas específicas de un concepto que queremos investigar y para su medición se utilizan los **Indicadores**, estos consisten en la cuantificación de las dimensiones de conceptos y construcción de métricas precisas. Es recomendable elaborar una lista lo más exhaustiva posible de indicadores para cada dimensión, siempre que sean significativos. En otras palabras, los indicadores son características observables de algo que son susceptibles de adoptar distintos valores o de ser expresadas en varias categorías. A continuación se presenta un ejemplo de esta matriz:

Matriz de Análisis de Auditoria de Red Empresa: ACME				
Objetivos				
General	Específicos	Dimensión	Indicadores	Instrumentos
Realizar una auditoría informática de red, en la empresa ACME, para la gestión de la interconexión de datos entre la Sede Central y Sucursales remotas.	Diagnosticar la situación actual de la gestión de la interconexión de datos entre la Sede Central y Sucursales remotas en la empresa ACME.	Organización	➢ Normas y políticas empresariales. ➢ Documentación técnica. ➢ Recursos humanos y materiales.	• Entrevistas. • Cuestionarios. • Encuestas. • Muestreos. • Técnicas de observación directa.
		Gestión	➢ Distribución de las funciones. ➢ Especificación de la plataforma y recursos. ➢ Software de Gestión de red. ➢ Técnicas de transferencia de datos.	
		Funcionamiento	➢ Identificación de equipos, topologías, servicios y distribución de la red. ➢ Disponibilidad de la conexión intranet e internet. ➢ Políticas de uso, mantenimiento y actualización técnica de la red.	
	Analizar los servicios de red entre la Sede Central y Sucursales remotas en la empresa ACME.	Servicios de Red	➢ Control de tráfico de red. ➢ Enrutamiento con menor consumo de recursos posible. ➢ Administración y control de seguridad de la red.	• Técnicas de observación Directa • Levantamiento de inventario • Técnicas de revisión documental • Cruce de información con estándares modelo OSI. • Software NetTools
	Analizar la información recolectada durante el proceso de Auditoría Informática de Redes.	Análisis de la información	➢ Resultados Obtenidos	
	Presentar un informe del proceso de Auditoría Informática de Redes.	Presentación de Informe	➢ Pre-Informe ➢ Informe Final	

Cuadro 3. Ejemplo: Matriz de Análisis de Auditoría.

En la matriz anterior se puede apreciar que las dimensiones son aspectos que queremos estudiar de los objetivos planteados y que los indicadores son elementos específicos de estos aspectos que pueden ser cuantificados, bien sea estableciendo controles para medirlos o mediante el uso de técnicas o software especiales de auditoría. Todos los elementos considerados en la matriz deben ser evaluados durante la fase de ejecución de la auditoría (Capítulo IV) para que el auditor pueda dar por finalizada esta etapa, si el auditor deja indicadores sin medir, no estará cubriendo en su totalidad los objetivos de la auditoría y por consiguiente los resultados no serán fidedignos en un 100%.

ESTRUCTURA DE DESGLOSE DEL TRABAJO

La Estructura de Desglose del Trabajo (EDT) es una de las herramientas de planeación más importantes en la administración de proyectos y consiste en desglosar nuestro proyecto en diferentes componentes o "entregables". Un **Entregable** puede ser definido como el resultado de un trabajo o una actividad y debe ser medible o cuantificable.

Para la elaboración del EDT se usa una estructura similar a un organigrama, el cual se desglosa generalmente en orden descendiente, de lo general a lo particular. Se trata de descomponer el proyecto o trabajo en entregables más fáciles de manipular.

En primera instancia se ubica el objetivo del proyecto, luego en un segundo nivel se colocan las componentes del proyecto y para cada una de estas componentes se detallan en niveles inferiores los productos, entregables paquetes de trabajo y actividades.

Es importante resaltar que la EDT no lleva ni secuencia ni duraciones ni tiempo, la EDT es una estructura que permite organizar el universo

entero del proyecto y posteriormente a la misma, se desprende la planeación detallada del tiempo y del costo. La EDT no lleva verbos, acciones ni tareas, se van a desprender a partir de ésta. La EDT va a estar compuesta por sustantivos o cualquier entregable del proyecto.

En un EDT deben aparecer todos los componentes que se tengan que llevar a cabo para alcanzar el objetivo principal del proyecto. La auditoría, puede gestionarse de forma similar a algún otro tipo de proyectos, por lo que también se pueden aplicar algunas de las técnicas utilizadas en la gerencia de proyectos.

Realizar un EDT de nuestra auditoría facilitará la construcción de otros instrumentos que serán estudiados más adelante.

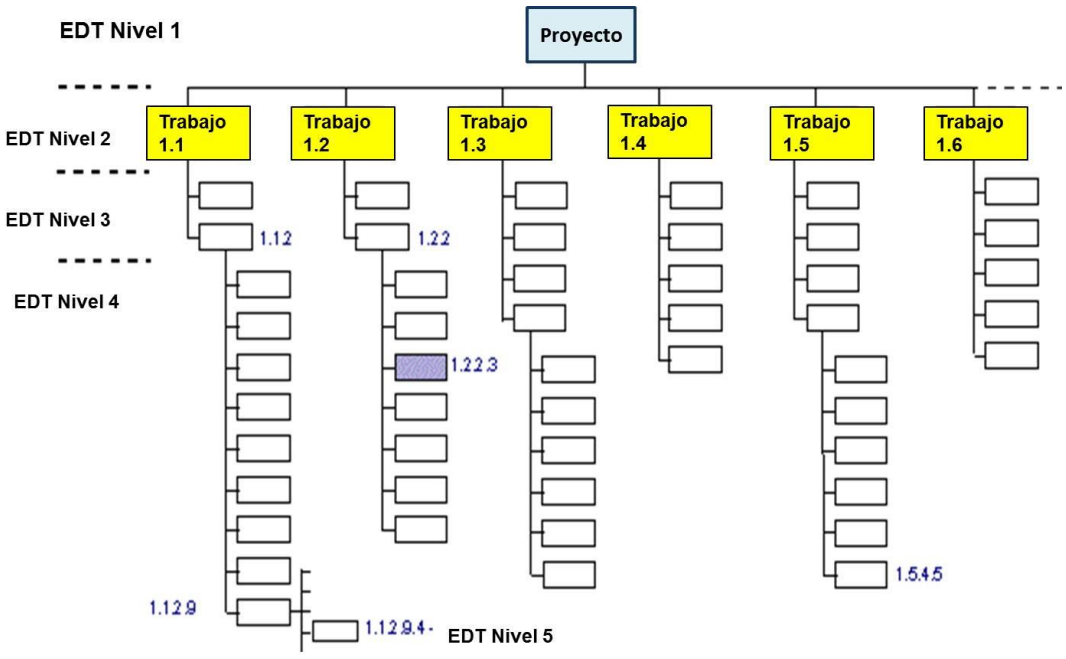


Figura 12. Estructura de Desglose del Trabajo (EDT).

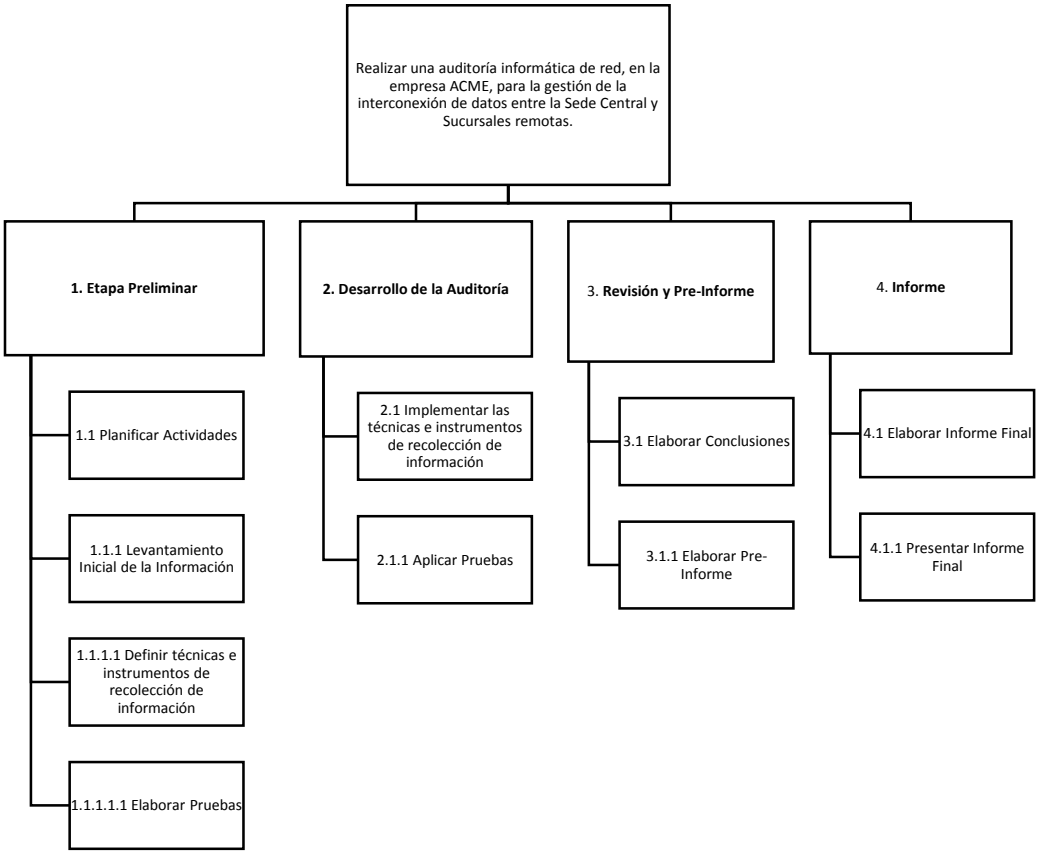


Figura 13. Ejemplo de una EDT.

PROGRAMA DE AUDITORÍA

Una vez realizado el EDT, es más fácil para el auditor organizar las actividades en forma de programa. En este programa es importante identificar la cantidad de horas estimadas para cada fase de la auditoría y los responsables de cada una de las actividades.

El programa de auditoría es algo bastante general, sin embargo deben incluirse todas las actividades. Las actividades van a depender de la construcción del EDT y a su vez el EDT se construye en base a las dimensiones e indicadores obtenidos de la matriz de análisis de auditoría, cuya construcción es posible una vez definido el alcance y los objetivos de la auditoría. Se evidencia que el proceso de auditoría es progresivo.

EMPRESA: ACME		FECHA: 03/06/2013	HOJA N° 1/1
FASE	**ACTIVIDAD**	**HORAS ESTIMADAS**	**ENCARGADOS**
I	**Etapa Preliminar:** • Planificación de actividades. • Levantamiento inicial de la información. • Definición de las técnicas e instrumentos de recolección de información.	40	• Ing. Germán Chávez • Ing. Manuel Castillo • Ing. Germán Chávez / Ing. Manuel Castillo
II	**Desarrollo de la Auditoría:** • Implementación de las técnicas e instrumentos de recolección de información.	60	• MSc. José Figueredo
III	**Revisión y Pre-Informe** • Conclusiones. • Elaboración del Pre-informe.	12	• Ing. Germán Chávez / Ing. Manuel Castillo / MSc. José Figueredo • Ing. Germán Chávez / Ing. Manuel Castillo / MSc. José Figueredo
IV	**Informe** • Elaboración del informe final. • Presentación del informe.	08	• Ing. Germán Chávez / Ing. Manuel Castillo / MSc. José Figueredo • Ing. Germán Chávez / Ing. Manuel Castillo / MSc. José Figueredo

Cuadro 4. Ejemplo: Programa de Auditoría.

CRONOGRAMA DE ACTIVIDADES

Posterior a la elaboración del cronograma de actividades, el siguiente paso lógico consiste en realizar un cronograma de actividades, el cual, básicamente muestra la ubicación de las actividades en semanas

correspondientes a la auditoría. Este cronograma puede construirse fácilmente con algún procesador de textos o algún gestor de hojas de cálculos.

			SEMANA			
	ACTIVIDADES	**RESPONSABLE**	**1**	**2**	**3**	**4**
1	Planificación de las actividades	Ing. Germán Chávez				
2	Levantamiento inicial de información.	Ing. Manuel Castillo				
3	Definición de las técnicas e instrumentos de recolección de información.	Ing. Germán Chávez / Ing. Manuel Castillo				
4	Implementación de las técnicas e instrumentos de recolección de información.	MSc. José Figueredo				
5	Conclusiones	Ing. Germán Chávez / Ing. Manuel Castillo / MSc. José Figueredo				
6	Elaboración del Pre- Informe	Ing. Germán Chávez / Ing. Manuel Castillo / MSc. José Figueredo				
7	Elaboración del informe final.	Ing. Germán Chávez / Ing. Manuel Castillo / MSc. José Figueredo				

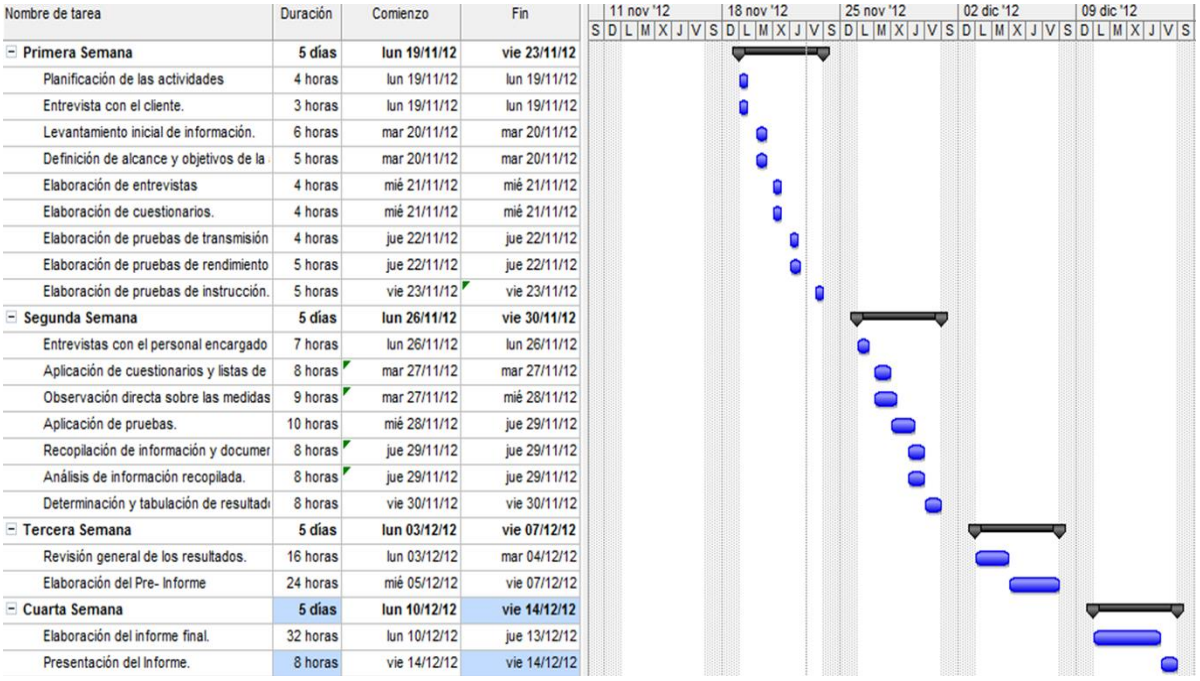
Cuadro 5. Ejemplo: Cronograma de Actividades.

DIAGRAMA DE GANTT

El diagrama de Gantt es una herramienta de planificación estratégica que permite al auditor exponer el tiempo de dedicación previsto para diferentes tareas o actividades a lo largo de un tiempo total determinado. A pesar de esto, el Diagrama de Gantt no indica las relaciones existentes entre actividades.

El Diagrama de Gantt se plantea en dos ejes: Un eje Horizontal Donde se define la escala de tiempo, un calendario adaptado a la unidad que mejor

se adapte al modelo de proyecto que estás llevando puede ser Día, Mes, Semana, Hora o año. En el eje Vertical Se plantea la tarea que se pretende ejecutar. Se muestra cómo una especie de barra horizontal que ocupará el tiempo necesario expresado en el eje horizontal. Entonces cada tarea se representa por una línea o barra en cada una de las filas del diagrama, mientras que las columnas representan el tiempo en distintas unidades (días, semanas, o meses) Dependiendo de la duración del proyecto. La fecha de inicio y la fecha de finalización de cada tarea, corresponden al inicio y final (respectivamente) de la barra correspondiente a esa actividad.



Nombre de tarea	Duración	Comienzo	Fin
Primera Semana	**5 días**	**lun 19/11/12**	**vie 23/11/12**
Planificación de las actividades	4 horas	lun 19/11/12	lun 19/11/12
Entrevista con el cliente.	3 horas	lun 19/11/12	lun 19/11/12
Levantamiento inicial de información.	6 horas	mar 20/11/12	mar 20/11/12
Definición de alcance y objetivos de la	5 horas	mar 20/11/12	mar 20/11/12
Elaboración de entrevistas	4 horas	mié 21/11/12	mié 21/11/12
Elaboración de cuestionarios.	4 horas	mié 21/11/12	mié 21/11/12
Elaboración de pruebas de transmisión	4 horas	jue 22/11/12	jue 22/11/12
Elaboración de pruebas de rendimiento	5 horas	jue 22/11/12	jue 22/11/12
Elaboración de pruebas de instrucción.	5 horas	vie 23/11/12	vie 23/11/12
Segunda Semana	**5 días**	**lun 26/11/12**	**vie 30/11/12**
Entrevistas con el personal encargado	7 horas	lun 26/11/12	lun 26/11/12
Aplicación de cuestionarios y listas de	8 horas	mar 27/11/12	mar 27/11/12
Observación directa sobre las medidas	9 horas	mar 27/11/12	mié 28/11/12
Aplicación de pruebas.	10 horas	mié 28/11/12	jue 29/11/12
Recopilación de información y documer	8 horas	jue 29/11/12	jue 29/11/12
Análisis de información recopilada.	8 horas	jue 29/11/12	jue 29/11/12
Determinación y tabulación de resultad	8 horas	vie 30/11/12	vie 30/11/12
Tercera Semana	**5 días**	**lun 03/12/12**	**vie 07/12/12**
Revisión general de los resultados.	16 horas	lun 03/12/12	mar 04/12/12
Elaboración del Pre- Informe	24 horas	mié 05/12/12	vie 07/12/12
Cuarta Semana	**5 días**	**lun 10/12/12**	**vie 14/12/12**
Elaboración del informe final.	32 horas	lun 10/12/12	jue 13/12/12
Presentación del Informe.	8 horas	vie 14/12/12	vie 14/12/12

Figura 14. Ejemplo de un Diagrama de Gantt.

Hay tareas que pueden ser simultáneas, consecutivas y hay tareas que pueden depender entre ellas, es decir si no se cumple una, no se puede dar inicio a la otra, hay también sub-tareas que son pequeñas actividades necesarias para cumplir una tarea.

La elaboración del diagrama de Gantt resulta muy sencilla y el auditor puede apoyarse en diferentes herramientas de software. Una de las herramientas más usadas a nivel mundial es Microsoft Poject, sin embargo, existen otras herramientas de software libre más livianas y gratuitas como Gantt Project que pueden descargarse rápidamente desde la página web del desarrollador.

Se puede apreciar que en el diagrama de Gantt se visualiza cada actividad con su respectiva duración en horas, lo cual facilita la tarea de calcular el presupuesto al auditor.

DIAGRAMA PERT-CPM

El diagrama PERT (Técnica de Revisión y Evaluación de Programas) es una representación gráfica de las relaciones entre las tareas del proyecto que permite calcular los tiempos del proyecto de forma sencilla.

Por otra parte el sistema CPM (Método del Camino Crítico) es utilizado para planear y controlar proyectos, añadiendo el concepto de costo al formato PERT. Para entender más fácilmente como se realiza este diagrama es importante conocer los siguientes términos:

- Nodo: puntos de unión de las ramas, que representa el momento en que comienza o termina una actividad.
- Ramas (o arcos): líneas que unen los nodos. Representan las actividades.
- Red: gráfica con un flujo en sus ramas
- Actividades Ficticias: sólo muestran relaciones de precedencia
- Holgura: diferencia entre el tiempo más lejano y el tiempo más cercano
- Ruta Crítica: ruta cuyas holguras son cero.

A continuación se muestra un ejemplo sobre la elaboración de un Diagrama PERT-CPM (Ejemplo con las actividades llevadas a cabo en la mañana, antes de salir de la casa).

PASO 1: Liste todas las actividades que va a llevar a cabo o a ejecutar, e identifíquelas con una etiqueta (preferiblemente una letra).

Etiqueta	Actividad	Duración	Precedencia
A	Despertarse		
B	Tender cama		
C	Cepillar dientes		
D	Afeitarme		
E	Bañarme		
F	Escoger ropa		
G	Vestirme		
H	Preparar desayuno		
I	Desayunar		
J	Ver noticias		
K	Salir		
L	Prender PC		
M	Revisar correo-e		
N	Apagar PC		

Figura 15. Paso 1, diagrama PERT-CPM.

PASO 2: Asigne la duración de cada actividad (en unidades de tiempo).

Etiqueta	Actividad	Duración	Precedencia
A	Despertarse	7	
B	Tender cama	2	
C	Cepillar dientes	2	
D	Afeitarme	5	
E	Bañarme	10	
F	Escoger ropa	5	
G	Vestirme	15	
H	Preparar desayuno	5	
I	Desayunar	10	
J	Ver noticias	60	
K	Salir	5	
L	Prender PC	1	
M	Revisar correo-e	30	
N	Apagar PC	1	

Figura 16. Paso 2, diagrama PERT-CPM.

PASO 3: Determine la precedencia o prelación de las actividades (se deben cumplir una vez finalizada una o más actividades o se pueden hacer simultáneamente).

Etiqueta	Actividad	Duración	Precedencia
A	Despertarse	7	-
B	Tender cama	2	E
C	Cepillar dientes	2	A
D	Afeitarme	5	C
E	Bañarme	10	D
F	Escoger ropa	5	M
G	Vestirme	15	F
H	Preparar desayuno	5	F
I	Desayunar	10	G, H
J	Ver noticias	60	A
K	Salir	5	I, N, J
L	Prender PC	1	D
M	Revisar correo-e	30	L, B
N	Apagar PC	1	M

Figura 17. Paso 3, diagrama PERT-CPM.

PASO 4: Proceda a graficar el Diagrama PERT. Normalmente se comienza de izquierda a derecha. Se emplean nodos para denotar inicio y fin de las actividades, líneas rectas horizontales (preferiblemente) para representar las actividades e identificadas con la etiqueta en la parte superior y la duración en la parte inferior.

Las actividades ficticias se dibujan con líneas discontinuas.

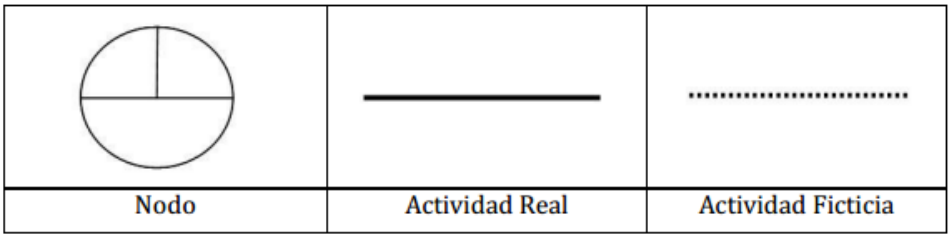


Figura 18. Notación, diagrama PERT-CPM.

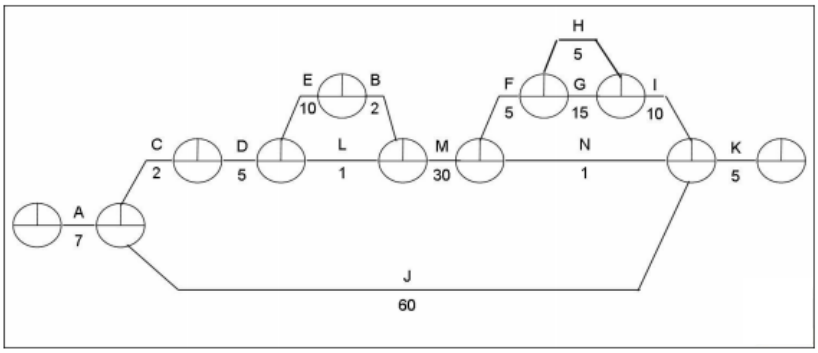


Figura 19. Paso 4, diagrama PERT-CPM.

PASO 5: Una vez que está graficado el PERT, se calculan los tiempos de ejecución de las actividades. Se comienza desde la izquierda, colocando el valor 0 en el cuadro izquierdo del primer nodo, y se va sumando el tiempo de duración de cada actividad para ir acumulando el tiempo. Cuando existan dos o más acumulados se toma el acumulado de mayor duración.

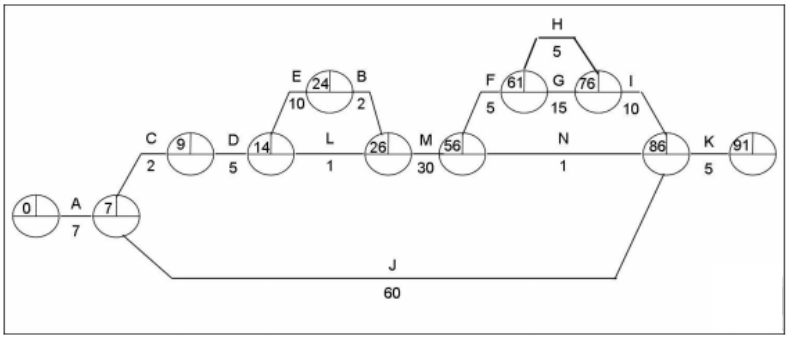


Figura 20. Paso 5, diagrama PERT-CPM.

PASO 6: Al terminar de calcular los tiempos de ejecución, se procede a calcular los tiempos de holgura, de derecha a izquierda. Se coloca en el cuadro derecho del último nodo el tiempo total del proyecto, y se va restando el tiempo de duración de cada actividad, para ir disminuyendo el tiempo. Cuando existan dos o más acumulados se toma el acumulado de menor duración.

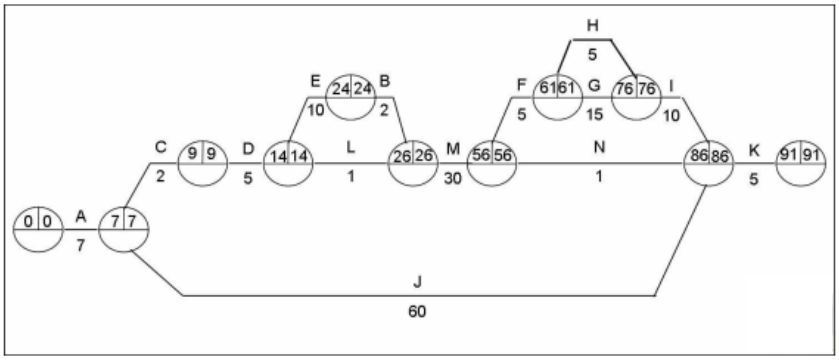


Figura 21. Paso 6, diagrama PERT-CPM.

PASO 7: Se calcula la ruta crítica, que pasa por los nodos donde el acumulado del cuadro de la izquierda es igual al acumulado del cuadro de la derecha. Normalmente se denota con un trazo más grueso o con otro color.

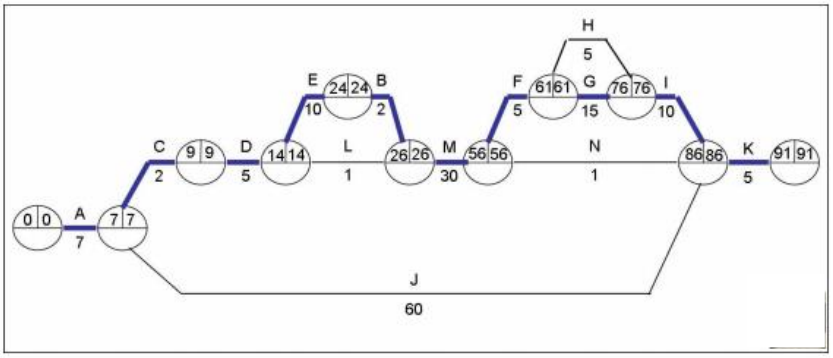


Figura 22. Paso 7, diagrama PERT-CPM.

Quizás el lector se dio cuenta que el proceso de auditoría puede ser realizado en su mayoría de forma secuencial, por lo que posiblemente no sea necesario realizar el diagrama PERT-CPM ya que la ruta crítica podría ser la única ruta que existe, pero igualmente ha sido incluido como una herramienta adicional que puede ser considerada por el auditor.

PRUEBAS

En la auditoría informática de sistemas de información, la prueba es el proceso de analizar un artículo del software para detectar la diferencia entre las condiciones existentes y requeridas, para evaluar las características de los artículos del software. Así pues, la prueba es el proceso de analizar un programa con el intento de encontrar errores. Este concepto puede generalizarse un poco más ya que se pueden realizar procedimientos para encontrar errores en el funcionamiento o configuración de las redes, en las bases de datos o en alguna de las otras áreas informáticas de la organización.

En la primera etapa de la auditoría es importante planificar los tipos de pruebas que serán realizadas para de esta forma estimar el tiempo y los recursos necesarios para las mismas. En el próximo capítulo se comentarán algunas de las pruebas que pueden realizarse para diferentes tipos de auditoría informática.

EXAMEN Y EVALUACIÓN DE LA INFORMACIÓN

En el capítulo anterior explicábamos un poco sobre los riesgos que pueden existir en las organizaciones, sin embargo la información también involucra algún tipo de riesgo (distorsión) que puede ocurrir por alguno de los siguientes motivos:

- Lejanía de la fuente de información.
- Prejuicios y motivos de quien suministra la información.
- Datos voluminosos.
- Operaciones cambiarias complejas.

Al existir el **Riesgo de la Información**, entonces existe también el **Riesgo de Auditoria**, el cual significa que el auditor acepta cierto nivel de

incertidumbre al realizar la auditoria. Este riesgo de auditoría está relacionado básicamente con tres (03) aspectos:

- Sobre la competencia de la evidencia.
- Sobre la estructura de control interno.
- Sobre la presentación de los Productos (Sistemas de Información).

El riesgo de auditoría al igual que los riesgos de la organización, tampoco puede ser eliminado del todo, pero puede ser mitigado considerablemente mediante el establecimiento de controles. A continuación se describen los principales tipos de riesgos de auditoría:

Riesgo de detección planeado: Existe al aplicar los programas de auditoria, cuyos procedimientos no sean suficientes para descubrir errores o irregularidades significativas.

Riesgo inherente: Evaluación de la probabilidad de que existan errores importantes en un segmento antes de considerar la eficiencia de la estructura de control interno.

Riesgo de control: Está asociado con la posibilidad de que los procedimientos de control interno, incluyendo a la unidad de auditoria interna, no puedan prevenir o detectar los errores e irregularidades significativas de manera oportuna.

Riesgo aceptable de auditoria: Medida de la disponibilidad del auditor para aceptar que la información contienen errores importantes después de terminada la auditoria y que ha emitido una opinión sin salvedad

HERRAMIENTAS (SOFTWARE)

El proceso de auditoría informática tiene la ventaja de que puede ser apoyado por el uso de distintos tipos de software para cada una de sus fases, muchas de estas herramientas pueden ser gratuitas o utilizarse en modo de evaluación durante el proceso de auditoría sin problema alguno. Pueden ser utilizados desde procesadores de textos para hacer el informe, programas diseñados para la gestión de proyectos, software especializado para realizar pruebas a cada una de las áreas a auditar, herramientas para el análisis de riesgos, entre otros.

Es importante que el auditor conozca los diferentes tipos de software que hay a disposición y las funciones que incorpora cada uno, de manera que pueda determinar dentro de la fase de planificación, cuáles de estas herramientas va a utilizar y los costos que la utilización de los mismos conlleva.

A continuación mencionaremos algunas herramientas por áreas que pueden ser bastante útiles al momento de realizar algún tipo de auditoría informática:

BASES DE DATOS

- DB Audit (Analizar bases de datos).

REDES

- NetTools (Monitoreo red, ancho de banda, calidad de conexión, etc.).
- PacketTracer (Simulador protocolos, seguimiento paquetes).
- Wireshark (Analizar paquetes de red).
- CommTraffic (Trafico de red).

- Netviz (Visualización).
- Free IP Tools (Monitorizar estado de la red).
- OSSTMM3 (Metodología)

ANÁLISIS DE RIESGOS

- @Risk
- Analyse de Risques Programmes
- AnalyZ
- AROME+
- BDSS (Bayesian Decision Support System
- BIS RISK ASSESSOR
- Buddy System
- COBRA (Consultative, Objective and Bi-functional Risk Analysis).
- CONTROL-IT
- CRAMM (CCTA Risk Analysis and Management Method)
- CRITI-CALC
- DDIS (Datenschutz-und-datensicherheits-informations-system).
- IS CASE
- LAVA (Los Alamos Vulnerability Analysis)
- LRAM & ALRAM
- MARION
- MELISA
- MINIRISK
- PREDICT
- PSICHE
- RANK-IT
- RISAN
- Risiko
- RiskCALC

- RiskPAC
- RiskWatch
- Security by Analysis (SBA)
- SISSI
- XRM (eXpert Risk Management)
- Xacta

GESTIÓN DE PROYECTOS (GANT, PERT-CPM, EDT)

- Microsoft Project.
- Gantt Project.
- Microsoft Visio.
- WBS Tool.
- WBS Chart Pro.

MONITOREO Y SOPORTE

- NetSupportManager (Control remoto estaciones de red).
- nVision (Monitoreo).
- Activity Monitor (Visualizar escritorios de estaciones en vivo).
- TeamViewer (Control remoto).

VIRTUALIZACIÓN

- VirtualBox (Varios Sistemas Operativos en un mismo ordenador).

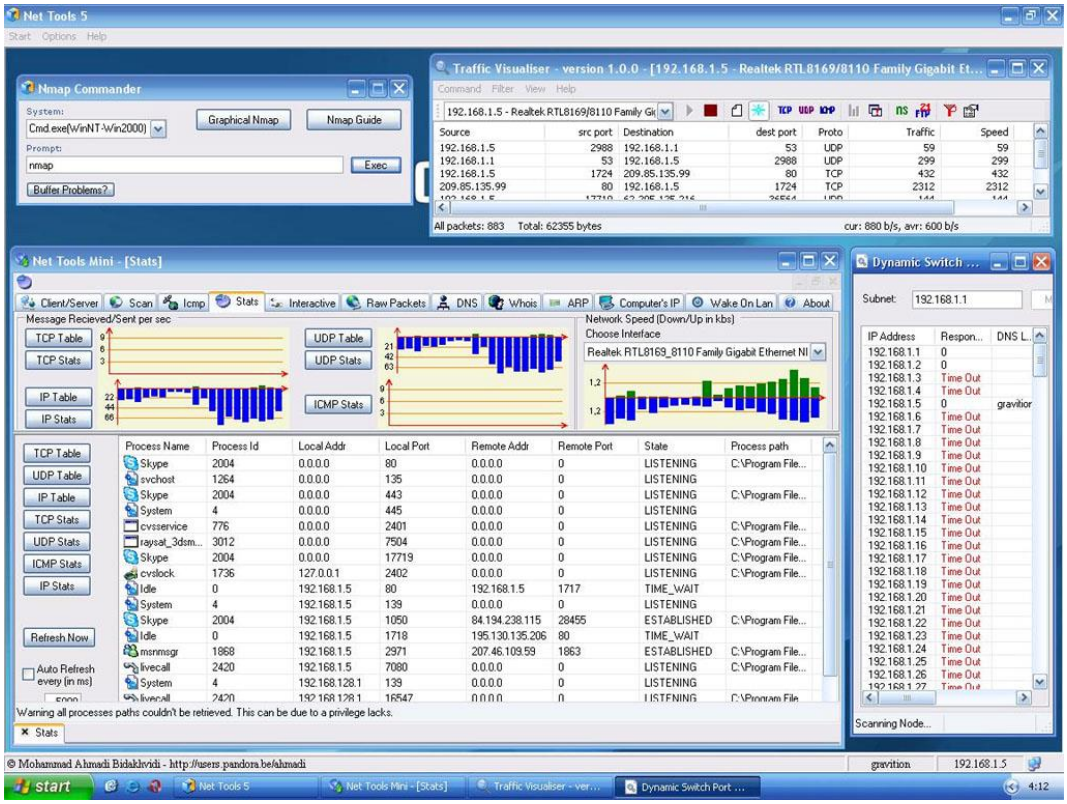


Figura 23. Ejemplo NetTools.

NOTAS DEL LECTOR

El lector puede aprovechar este espacio para escribir algunas notas relacionadas con los tópicos estudiados en este capítulo.

CAPÍTULO IV

FASE II: EJECUCIÓN DE LA AUDITORÍA

La segunda fase de la auditoría consiste en realizar las actividades descritas en la fase de planificación. Es una etapa más técnica, sin embargo se hace fácil su realización ya que se debe seguir el programa de auditoría.

Esta fase se centra en la Evaluación del Control Interno Informático y por lo general se realizan las siguientes actividades:

- Diseño de Cuestionarios.
- Diseño de Pruebas.
- Evaluación de Riesgos.
- Listas de Chequeo.
- Aplicación de Instrumentos.
- Tabulación de los Datos.
- Evaluación y Análisis de la Información.
- Determinación de los Hallazgos de Auditoria.

El auditor debe recopilar toda la información relevante al proceso de auditoría durante esta etapa y debe solicitar a la organización la documentación necesaria, desde los niveles gerenciales hasta los niveles operativos para de esta manera, conocer el funcionamiento de la organización a fin de evaluar si los procedimientos se realizan de la forma en que se describen en sus documentos.

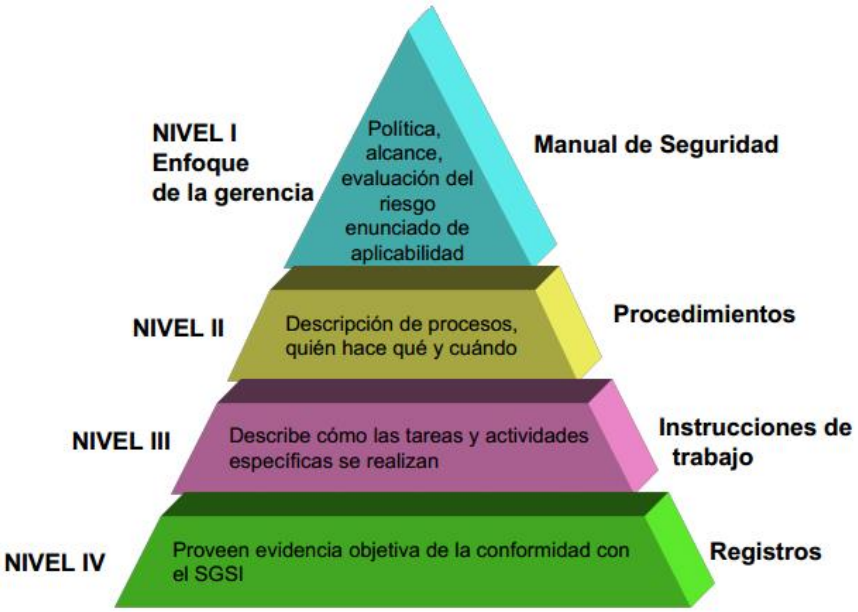


Figura 24. Documentación Requerida.

DISEÑO DE CUESTIONARIOS

Un cuestionario es un juego formalizado de las preguntas para obtener la información de encuestados. Debe traducir la información necesaria en un conjunto de preguntas específicas a las que los encuestados pueden responder y arrojen información. Un cuestionario debe animar, motivar, y apoyar al encuestado a comprometerse en la entrevista, cooperar, y a completarla. Un cuestionario debe minimizar el error de respuesta.

Mediante el uso de cuestionarios, el auditor puede hacer gran parte del levantamiento de la información. Es importante que el auditor diseñe bien los cuestionarios, las preguntas deben redactarse en base a los indicadores que desea medir.

Preguntas sin estructura: Las preguntas poco estructuradas son las preguntas abiertas a las que los encuestados responden en sus propias palabras.

Preguntas estructuradas: Las preguntas estructuradas especifican el conjunto de alternativas de respuesta y formato de respuesta. Una pregunta estructurada podría ser examen de opción múltiple, dicotómica, o de escala.

Preguntas de selección múltiple: En las preguntas de selección múltiple, el investigador provee una elección de las respuestas y los encuestados son invitados a seleccionar uno o más de las alternativas dadas.

Preguntas dicotómicas: Preguntas estructurada con sólo dos alternativas de respuesta, como sí o no. A menudo, las dos alternativas de interés son complementadas por una alternativa neutra, como "Ninguna opinión", "No lo sé", "Ambos", o "Nada."

DISEÑO DE PRUEBAS

El auditor debe diseñar las pruebas correspondientes al proceso de auditoría. Es necesario que se tomen en cuenta todos los aspectos que serán evaluados y se defina el orden y las herramientas que serán implementadas. Todas las pruebas deben ser notificadas a la organización y se deben tomar las medidas preventivas en caso de que las pruebas afecten el funcionamiento de la organización. En esta misma etapa, el auditor debe seleccionar los controles que utilizará para medir los indicadores de la matriz de análisis de auditoría.

EVALUACIÓN DE RIESGOS

En esta etapa se realiza el respectivo análisis de riesgos, para lo cual se construye la llamada matriz de riesgos. Consiste en una lista de los principales riesgos que corren los recursos informáticos de la organización,

para los cuales se establece la probabilidad de que ocurran y el impacto que causaría a la organización cada uno de ellos. Para realizar esta ponderación, el auditor establece previamente los parámetros entre los cuales estarán los resultados. Para el análisis de riesgos, pueden utilizarse algunas de las herramientas o metodologías que fueron mencionadas en el capítulo anterior.

MATRIZ DE RIESGOS

Existen varias formas de elaborar la matriz de riesgos, a continuación presentaremos un ejemplo bastante sencillo:

Descripción	Impacto	Probabilidad
Incendio	3	1
Inundación	2	1
Vulnerabilidad remota	2	2
Accesos indebidos	3	3
Accesos no autorizados al Data center	3	2
Tendido eléctrico junto con tendido de red	2	2
Uso de contraseñas no seguras	2	3

Cuadro 6. Ejemplo: Matriz de Riesgos.

Impacto:

1) Bajo
2) Medio
3) Alto

Probabilidad:

1) Bajo
2) Medio
3) Alto

Otro ejemplo un poco más elaborado del diseño de la matriz de riesgos:

CONTROL DE VERSIONES					
Versión	*Hecha por*	*Revisada por*	*Aprobada por*	*Fecha*	*Motivo*

IDENTIFICACIÓN Y EVALUACIÓN CUALITATIVA DE RIESGOS

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO

PROBABILIDAD	VALOR NUMÉRICO	IMPACTO	VALOR NUMÉRICO
Muy Improbable	0.1	Muy Bajo	0.05
Relativamente Probable	0.3	Bajo	0.10
Probable	0.5	Moderado	0.20
Muy Probable	0.7	Alto	0.40
Casi Certeza	0.9	Muy Alto	0.80

TIPO DE RIESGO	PROBABILIDAD X IMPACTO
Muy Alto	Mayor a 0.50
Alto	Menor a 0.50
Moderado	Menor a 0.30
Bajo	menor a 0.10
Muy Bajo	Menor a 0.05

CÓDIGO DEL RIESGO	DESCRIPCIÓN DEL RIESGO	CAUSA RAÍZ	TRIGGER	ENTREGABLES AFECTADOS	ESTIMACIÓN DE PROBABILIDAD	OBJETIVO AFECTADO	ESTIMACIÓN DE IMPACTO	PROB X IMPACTO	TIPO DE RIESGO
						Alcance			
						Tiempo			
						Costo			
						Calidad			
						TOTAL PROBABILIDAD X IMPACTO			
						Alcance			
						Tiempo			
						Costo			
						Calidad			
						TOTAL PROBABILIDAD X IMPACTO			

Figura 25. Matriz de Riesgos.

Después de haber realizado la matriz de riesgos, el auditor debería realizar un análisis de los resultados obtenidos. Para visualizar más fácilmente los resultados, el auditor puede apoyarse en la elaboración de gráficas.

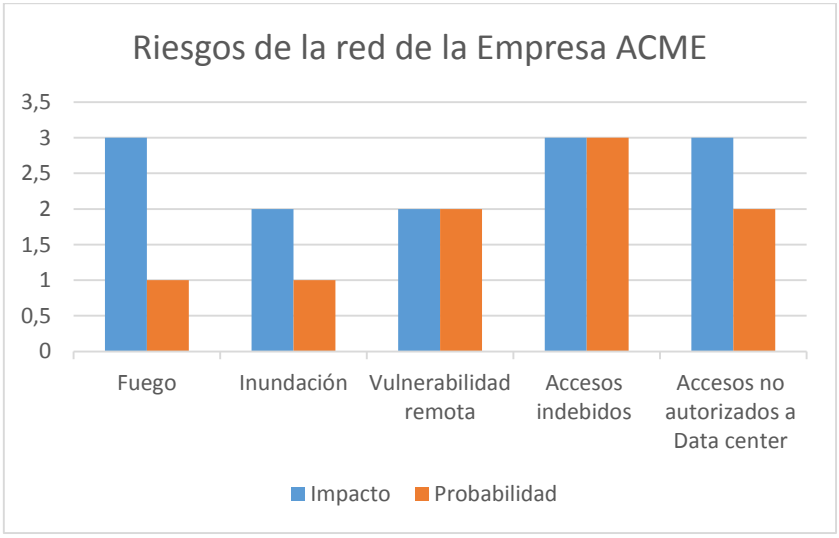


Figura 26. Gráfico de la Matriz de Riesgos.

Análisis:

De la matriz de riesgo se puede notar claramente el alto impacto de los principales peligros a la estabilidad y correcto funcionamiento de la red del grupo metropolitano, en este caso:

- Incendio
- Accesos indebidos
- Accesos no autorizados a data center

Se puede inferir dado los resultados obtenidos, la necesidad de dedicar mayores esfuerzos a mitigar estos riegos y de esta forma prevenir su materialización en el futuro.

LISTAS DE CHEQUEO

Las Listas de Control, Check Lists u Hojas de Verificación, son formatos creados para realizar actividades repetitivas, controlar el cumplimiento de una lista de requisitos o recolectar datos ordenadamente y de forma sistemática. Se usan para hacer comprobaciones sistemáticas de actividades o productos asegurándose de que el auditor no se olvida de nada importante.

Los usos principales de las listas de chequeo son los siguientes:

- Realización de actividades en las que es importante que no se olvide ningún paso y/o deben hacerse las tareas con un orden establecido.
- Realización de inspecciones donde se debe dejar constancia de cuáles han sido los puntos inspeccionados.
- Examinar o analizar la localización de defectos. Verificar las causas de los defectos.

- Verificación y análisis de operaciones.
- Recopilar datos para su futuro análisis.

En definitiva, estas listas suelen ser utilizadas para la realización de comprobaciones rutinarias y para asegurar que al operario o el encargado de dichas comprobaciones no se le pasa nada por alto, además de para la simple obtención de datos.

La ventaja de los check lists es que, además de sistematizar las actividades a realizar, una vez rellenados sirven como registro, que podrá ser revisado posteriormente para tener constancia de las actividades que se realizaron en un momento dado.

Es importante que las listas de control queden claramente establecidas e incluyan todos los aspectos que puedan aportar datos de interés para la organización. Es por ello preciso que quede correctamente recogido en la lista de control:

- Qué tiene que controlarse o chequearse.
- Cuál es el criterio de conformidad o no conformidad (qué es lo correcto y qué lo incorrecto).
- Cada cuánto se inspecciona: frecuencia de control o chequeo.
- Quién realiza el chequeo y cuáles son los procedimientos aplicables.

Conviene, por último, que se disponga de un apartado de observaciones con el fin de poder obtener información previa sobre posibles motivos que han causado la disconformidad.

EJECUCIÓN DE LA AUDITORIA

Procedimientos de auditoria Informática de Red				Sección de Trabajo PAGINA 1 de 1			
Empresa: ACME							
Unidad y/o departamento: Sistemas							
Área: Plataforma – Redes							
Periodo de revisión desde	**03**	**06**	**2013**	**Hasta:**	**21**	**06**	**2013**

Nº	Descripción	Sí	No	N/A	Observaciones
1	Realice las encuestas	x			
2	Aplique cuestionario de Control Interno	x			
3	Aplique lista de Chequeo	x			
4	Llene Matriz de Riesgos	x			
5	Realizar Pruebas (Monitoreo – Transmisión)	x			
6	Examen y evaluación de la información	x			
7	Realice análisis de riesgos	x			
8	Especifique evidencias de auditoría	x			
9	Tabule Resultados	x			
10	Análisis de Resultados	x			

Cuadro 7. Ejemplo: Lista de Chequeo de auditoría.

APLICACIÓN DE INSTRUMENTOS

El próximo paso en nuestra secuencia de auditoría consiste en aplicar todos los instrumentos que han sido elaborados cuidadosamente para tal fin. El auditor debe tomarse el tiempo necesario para aplicar las pruebas planificadas. Una vez realizados estos procedimientos, el auditor debe analizar y sintetizar todos los resultados obtenidos para pasar a la siguiente fase de la auditoría (Capítulo V).

TABULACIÓN DE LOS RESULTADOS

Para la Tabulación de los resultados obtenidos se deben seguir los siguientes procedimientos:

PASO 1: Se debe graficar por dimensión e indicador, y la gráfica debe reflejar el resultado en términos porcentuales y presentar el resultado por cada grupo de tres preguntas.

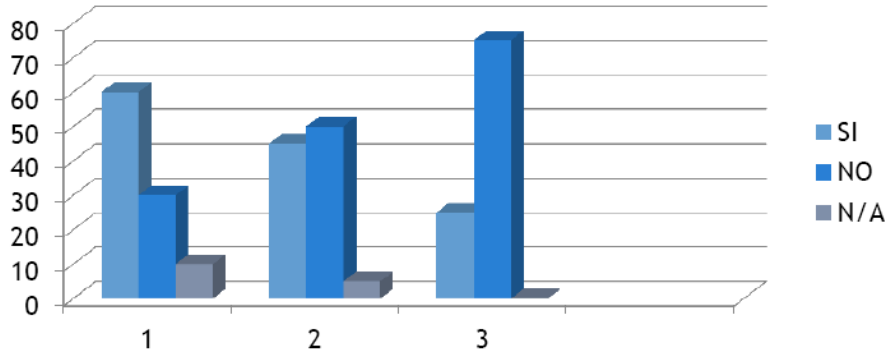


Figura 27. Ejemplo: Gráfico.

PASO 2: Debajo de cada gráfico debe realizarse un comentario de análisis e inferir, es decir, se piensa, se estima etc. las consecuencias de los resultados (Recuerda: el Auditor solo comenta en términos de inferencias no asevera nada).

PASO 3: Para tabular los resultados de una entrevista debe utilizarse la técnica de análisis de contenidos.

MATRIZ DE ANALISIS DE CONTENIDO-ENTREVISTA E01		
Pregunta	**Respuesta**	**Recomendación**
1.		
2.		

Cuadro 8. Ejemplo: Matriz de Análisis de Contenidos.

PASO 4: En el caso de la matriz de riesgo, según la valoración realizada de los riesgos, debe comentar los resultados obtenidos, realizando las inferencias correspondientes.

PASO 5: En el caso de pruebas con el uso de software, muchos de ellos al aplicarlos, arrojan resultados en informes que constituyen evidencia de auditoría, en caso de que no generen ningún informe, queda a juicio del auditor elaborar su propio formato.

EVALUACIÓN Y ANÁLISIS DE LA INFORMACIÓN

Para lograr el cumplimiento de esta etapa, se requiere que el auditor tenga dominio del área que está auditando (redes, bases de datos, otras), para que pueda interpretar los resultados arrojados por el software y tener criterio para realizar la evaluación. Se recomienda a los estudiantes que se aventuran a realizar la auditoría como trabajo especial de grado, solicitar la asesoría de algún profesor u otro profesional que tenga conocimientos especializados en las áreas necesarias. La idea de solicitar esta asesoría no consiste en que el tutor realice la evaluación, sino que sirva para aclarar algunos conceptos o resultados. Por ejemplo, algún software podría arrojarnos que el ancho de banda disponible es X, el auditor debe saber interpretar que significa el valor de X y evaluar si es positivo o negativo para

el funcionamiento de la organización, si el auditor no sabe hacer esta "traducción" lo ideal sería buscar apoyo en lugar de omitir el resultado o hacer conjeturas erróneas.

DETERMINACIÓN DE LOS HALLAZGOS DE AUDITORIA

Para que el auditor maneje los hallazgos o resultados de la auditoría de forma organizada, recomendamos utilizar el siguiente formato para cada uno de los procesos a auditar:

LOGO DE LA FIRMA

PROGRAMA DE AUDITORÍA

PROCESO A AUDITAR:

N°	PROCEDIMIENTO DE AUDITORÍA	CUMPLE	NO CUMPLE	REFERENCIAS	OBSERVACIONES

Cuadro 9. Formato Programa de Auditoría.

En la primera columna se establece una identificación, en la siguiente columna se listan los procedimientos de auditoría (normalmente basándose en controles), posteriormente se coloca si cumple o no cumple (si cumple a medias, entonces no cumple), en las referencias se puede colocar el control que se está utilizando para evaluar y por último las observaciones sobre la situación con respecto a ese control. Normalmente las observaciones se colocan cuando no se cumple el control, sin embargo, el auditor puede colocar observaciones a pesar de que el control se cumple, pero podría ser mejorado.

PROGRAMA DE AUDITORÍA

PROCESO A AUDITAR: Revisión de los derechos de acceso al usuario
OBJETIVO: Verificar los riesgos asociados a la Revisión de los derechos de acceso al usuario en los equipos de redes e interconexión del Grupo Metropolitano

N°	PROCEDIMIENTO DE AUDITORÍA	CUMPLE	NO CUMPLE	REFERENCIAS	OBSERVACIONES
1	Verificar la existencia de un programa para la revisión de los derechos de acceso de los usuarios a intervalos regulares.		X	ISO 27002:2005 11.2.4.A	LA ORGANIZACIÓN NO CUENTA CON UN PROGRAMA PARA LA REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS A INTERVALOS REGULARES, PERO SI EXISTEN POLÍTICAS PARA LA INMEDIATA MODIFICACIÓN O ELIMINACIÓN DE DERECHOS DE ACCESO DE LOS USUARIOS EN CASO DE ASCENSOS O TERMINACIÓN DEL EMPLEO RESPECTIVAMENTE.
2	Verificar el cumplimiento del programa para la revisión de los derechos de acceso de los usuarios a intervalos regulares.		X	ISO 27002:2005 11.2.4.A	NO SE CUMPLE LA REVISIÓN DE LOS DERECHOS DE USUARIOS PERIÓDICAMENTE, SOLO EN LOS CASOS MENCIONADOS EN LA OBSERVACIÓN ANTERIOR.
3	Verificar la existencia de un protocolo para la revision y reasignación de derechos de acceso del usuario cuando se traslada de un empleo a otro dentro de la misma organización	X		ISO 27002:2005 11.2.4.B	LA ORGANIZACIÓN CUENTA CON UN PROTOCOLO PARA LA REVISIÓN Y REASIGNACIÓN DE DERECHOS DE ACCESO DEL USUARIO CUANDO SE TRASLADA DE UN EMPLEO A OTRO DENTRO DE LA MISMA ORGANIZACIÓN. EL GERENTE DEL ÁREA A DONDE ES TRASLADADO EL EMPLEADO NOTIFICA AL DEPARTAMENTO DE SISTEMAS SOBRE EL NUEVO CARGO QUE OCUPARÁ Y EL NIVEL DE ACCESO QUE LE DEBERÁ SER OTORGADO. INMEDIATAMENTE SE BLOQUEAN LOS DERECHOS DE ACCESO ANTERIORES Y SE OTORGAN LOS NUEVOS.
4	Verificar el cumplimiento del protocolo para la revision y reasignación de derechos de acceso del usuario cuando se traslada de un empleo a otro dentro de la misma organización	X		ISO 27002:2005 11.2.4.B	EL PROTOCOLO SE CUMPLE CABALMENTE, SIEMPRE QUE EL GERENTE ENCARGADO DEL ÁREA A DONDE ES TRASLADADO EL EMPLEADO NOTIFIQUE OPORTUNAMENTE.
5	Verificar la existencia de un programa para la revisión de las autorizaciones para derechos de acceso privilegiados especiales.		X	ISO 27002:2005 11.2.4.C	LA ORGANIZACIÓN NO CUENTA CON UN PROGRAMA PARA LA REVISIÓN DE LAS AUTORIZACIONES PARA DERECHOS DE ACCESO PRIVILEGIADOS ESPECIALES. LOS DERECHOS DE ACCESO PRIVILEGIADOS ESPECIALES SON AUTORIZADOS O RESTRINGIDOS POR EL GERENTE DE SISTEMAS.
6	Verificar el cumplimiento del programa para la revisión de las autorizaciones para derechos de acceso privilegiados especiales a intervalos más frecuentes.		X	ISO 27002:2005 11.2.4.C	NO SE CUMPLE UNA REVISIÓN PERIÓDICA DE LAS AUTORIZACIONES LOS DERECHOS PRIVILEGIADOS ESPECIALES.
7	Verificar la existencia de un procedimiento para chequear la asignación de privilegios a intervalos regulares para asegurar que no se hayan obtenido privilegios no autorizados.		X	ISO 27002:2005 11.2.4.D	NO EXISTE UN PROGRAMA PARA CHEQUEAR A INTERVALOS REGULARES LA ASIGNACION DE PRIVILEGIOS PARA ASEGURAR QUE NO SE HAYAN OBTENIDO PRIVILEGIOS NO AUTORIZADOS. SOLO SE CHEQUEAN ESTOS PRIVILEGIOS BAJO SOSPECHA DE QUE SE HAN OBTENIDO PRIVILEGIOS NO AUTORIZADOS.
8	Verificar el cumplimiento del procedimiento para chequear la asignación de privilegios para asegurar que no se hayan obtenido privilegios no autorizados.		X	ISO 27002:2005 11.2.4.D	NO SE CUMPLE UN PROCEDIMIENTO PERIÓDICO PARA REVISAR ESTOS PRIVILEGIOS.
9	Verificar la existencia de una metodología para registrar los cambios en las cuentas privilegiadas para una revisión periódica.		X	ISO 27002:2005 11.2.4.E	LA ORGANIZACIÓN NO CUENTA CON UNA METODOLOGÍA PARA REGISTRAR LOS CAMBIOS EN LAS CUENTAS PRIVILEGIADAS PARA UNA REVISIÓN PERIÓDICA.
10	Verificar el debido registro de los cambios en las cuentas privilegiadas para una revisión periódica.		X	ISO 27002:2005 11.2.4.E	LOS CAMBIOS SON REALIZADOS PERO NO SE DEJA NINGÚN DOCUMENTO ESCRITO.

Realizado por: DAI Consultores C.A
ING. HERNAYS ALVAREZ
ING. ALBERT DURAN
ING. RAFAEL LINAREZ
ING. JULIO CASTILLO

Cuadro 10. Ejemplo: Hallazgos.

Las observaciones recopiladas en el instrumento anterior, servirán de base para redactar los hallazgos que se incluirán en el informe final (ver Capítulo V). En base a estos hallazgos el auditor deberá realizar algunas recomendaciones a la organización, a continuación se presenta un formato que puede ser bastante útil para este fin:

Referencia	Recomendaciones	Acciones Correctivas

Cuadro 11. Formato Recomendaciones.

En la primera columna se coloca la identificación correspondiente al control que se utilizó en el formato anterior, luego se colocan las recomendaciones y el período de tiempo para realizar las acciones correctivas.

Referencia	Recomendaciones	Acciones Correctivas
1	SE RECOMIENDA AL GERENTE DE SISTEMAS QUE SE ELABORE UN PROGRAMA PARA LA REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS A INTERVALOS TRIMESTRALES. ESTO SERIA BENEFICIOSO DEBIDO A QUE COMPLEMENTARÍA LAS POLÍTICAS PARA LA INMEDIATA MODIFICACIÓN O ELIMINACIÓN DE DERECHOS DE ACCESO DE LOS USUARIOS EN CASO DE ASCENSOS O TERMINACIÓN DEL EMPLEO RESPECTIVAMENTE Y MITIGARÍA EL RIESGO DE ACCESOS INDEBIDOS.	EL DEPARTAMENTO DE SISTEMA SE COMPROMETE AL DESARROLLO DE ESTE PLAN EN UN PLAZO NO MAYOR A 30 DÍAS CONTINUOS.
5	SE RECOMIENDA AL GERENTE DE SISTEMAS QUE SE ELABORE UN PROGRAMA PARA LA REVISIÓN DE LAS AUTORIZACIONES PARA DERECHOS DE ACCESO PRIVILEGIADOS ESPECIALES A INTERVALOS MENSUALES. ESTO EN PRO DE PRESERVAR LA SEGURIDAD DE LAS ÁREAS CRÍTICAS.	EL DEPARTAMENTO DE SISTEMA SE COMPROMETE AL DESARROLLO DE ESTE PLAN EN UN PLAZO NO MAYOR A 30 DÍAS CONTINUOS.
7	SE RECOMIENDA A LA GERENCIA DE SISTEMAS, ELABORAR UN PROGRAMA PARA CHEQUEAR A INTERVALOS REGULARES LA ASIGNACION DE PRIVILEGIOS PARA ASEGURAR QUE NO SE HAYAN OBTENIDO PRIVILEGIOS NO AUTORIZADOS. ESTO AYUDARÍA A MITIGAR EL RIESGO DE ACCESOS INDEBIDOS POR PARTE DEL PERSONAL DE LA ORGANIZACIÓN.	EL DEPARTAMENTO DE SISTEMA SE COMPROMETE AL DESARROLLO DE ESTE PLAN EN UN PLAZO NO MAYOR A 30 DÍAS CONTINUOS.
9	SE RECOMIENDA AL GERENTE DE SISTEMAS, ELABORACIÓN E IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA REGISTRAR LOS CAMBIOS EN LAS CUENTAS PRIVILEGIADAS PARA UNA REVISIÓN PERIÓDICA. ESTO SERÍA DE GRAN UTILIDAD AL MOMENTO DE REVISAR LA PERMISOLOGÍA Y LOS DERECHOS DE ACCESO DE ALGÚN USUARIO.	EL DEPARTAMENTO DE SISTEMA SE COMPROMETE AL DESARROLLO DE ESTE PLAN EN UN PLAZO NO MAYOR A 30 DÍAS CONTINUOS.

Cuadro 12. Ejemplo: Recomendaciones.

PAPELES DE TRABAJO

Los papeles de trabajo son registros que conserva el auditor sobre los procedimientos aplicados, las pruebas realizadas, la información obtenida y las conclusiones pertinentes.

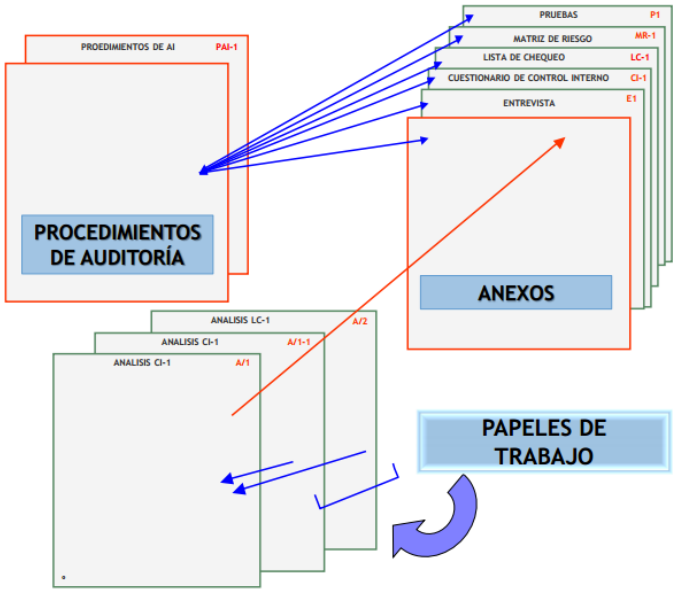


Figura 28. Papeles de Trabajo.

AUDITORÍA INFORMÁTICA DE SISTEMAS

En esta sección se tratará de orientar al lector sobre el proceso de auditoría de sistemas de información que ya están funcionando en la organización. Usualmente se realiza este tipo de auditoría cuando el sistema ha presentado inconsistencias o se sospecha que alguna parte del sistema se ha degenerado (módulos, base de datos, archivos).

En este caso, el auditor debe documentarse sobre el funcionamiento del sistema, sólo de esta forma podrá planificar las pruebas y así evaluar el funcionamiento para poder dar algún veredicto. Cuando no se tiene acceso al código fuente o la documentación del software (modelos), se realizan las

llamadas **Pruebas de Caja Negra**. En este tipo de prueba, el auditor sabe las entradas y qué los resultados previstos deben ser, pero no necesariamente cómo el programa llegó ellas. La prueba de caja negra se refiere a veces como la prueba funcional.

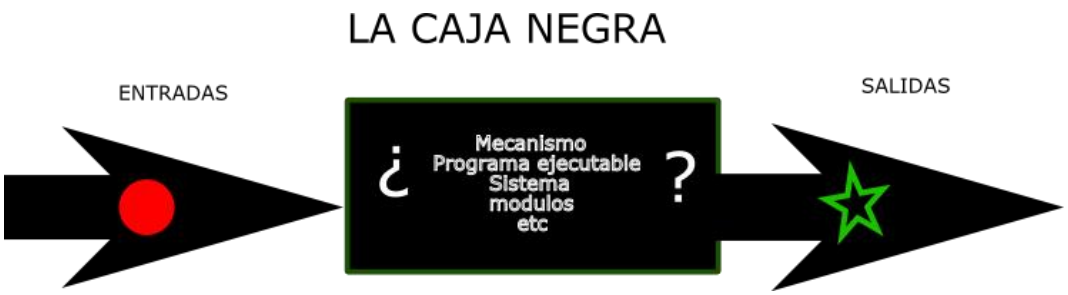


Figura 29. Pruebas de Caja Negra.

Los casos de la prueba para la prueba de caja negra se idean normalmente tan pronto como las especificaciones del programa sean completas. Los casos de la prueba se basan en clases de equivalencia. Existen varios tipos de pruebas de caja negra, tales como:

Pruebas de Consentimiento: Consiste en determinar si los controles internos operan como fueron diseñados para operar.

Pruebas de Controles del Usuario: Se realizan mediante cuestionarios, entrevistas, observación y evaluaciones hechas directamente a los usuarios.

Pruebas Sustantivas: El objetivo es obtener evidencia suficiente que permita al auditor emitir su juicio en las conclusiones acerca de cuándo pueden ocurrir pérdidas materiales durante el procesamiento de la información. Estas pruebas pueden ser:

- Pruebas para identificar errores en el procesamiento o de falta de seguridad o confidencialidad.

- Pruebas para asegurar la calidad de los datos.
- Pruebas para identificar la inconsistencia de los datos.
- Pruebas para comparar con los datos o contadores físicos.
- Confirmación de datos con fuentes externas.
- Pruebas para confirmar la adecuada comunicación.
- Pruebas para determinar la falta de seguridad.
- Pruebas para determinar problemas de legalidad.

Muchos autores consideran que estas pruebas permiten encontrar:

- Funciones incorrectas o ausentes.
- Errores de interfaz.
- Errores en estructuras de datos o en accesos a las Bases de Datos externas.
- Errores de rendimiento.
- Errores de inicialización y terminación.

Para preparar los casos de pruebas hacen falta un número de datos que ayuden a la ejecución de los estos casos y que permitan que el sistema se ejecute en todas sus variantes, pueden ser datos válidos o inválidos para el programa según si lo que se desea es hallar un error o probar una funcionalidad. Los datos se escogen atendiendo a las especificaciones del problema, sin importar los detalles internos del programa, a fin de verificar que el programa corra bien.

Para desarrollar la prueba de caja negra existen varias técnicas, entre ellas están:

- **Técnica de la Partición de Equivalencia:** esta técnica divide el campo de entrada en clases de datos que tienden a ejercitar determinadas funciones del software.

- **Técnica del Análisis de Valores Límites:** esta Técnica prueba la habilidad del programa para manejar datos que se encuentran en los límites aceptables.
- **Técnica de Grafos de Causa-Efecto:** es una técnica que permite al encargado de la prueba validar complejos conjuntos de acciones y condiciones.

Dentro del método de Caja Negra, la técnica de la Partición de Equivalencia es una de las más efectivas pues permite examinar los valores válidos e inválidos de las entradas existentes en el software, descubre de forma inmediata una clase de errores que, de otro modo, requerirían la ejecución de muchos casos antes de detectar el error genérico. La partición equivalente se dirige a la definición de casos de pruebas que descubran clases de errores, reduciendo así en número de clases de prueba que hay que desarrollar.

PROCEDIMIENTOS DE PRUEBA

Un procedimiento de prueba específica como realizar uno o varios casos de prueba o parte de estos. Por ejemplo un procedimiento de prueba puede ser una instrucción para un individuo sobre cómo ha de realizar un caso de prueba manualmente, o puede ser una especificaron de cómo interaccionar manualmente con una herramienta de automatización de pruebas para crear componentes ejecutables de pruebas.

COMPONENTES DE PRUEBA

Un componente de prueba automatiza uno o varios procedimientos de prueba o parte de ellos. Los componentes de pruebas pueden ser desarrollados utilizando lenguaje de guiones o un lenguaje de programación o pueden ser grabados con una herramienta de automatización de pruebas.

Los componentes de pruebas se utilizan para probar los componentes en el modelo de implementación proporcionando entradas de prueba, controlando y monitorizando la ejecución de los componentes a probar y, posiblemente informando de los resultados de las pruebas.

PLAN DE PRUEBA

El propósito del plan de pruebas es dejar de forma explícita el alcance, el enfoque, los recursos requeridos, el calendario, los responsables y el manejo de riesgos de un proceso de pruebas.

Está constituido por un conjunto de pruebas. Cada prueba debe:

- Dejar claro qué tipo de propiedades se quieren probar (corrección, robustez, fiabilidad, amigabilidad).
- Dejar claro cómo se mide el resultado.
- Especificar en qué consiste la prueba (hasta el último detalle de cómo se ejecuta).
- Definir cuál es el resultado que se espera (identificación, tolerancia).

Las pruebas carecen de utilidad, tanto, sí no se sabe exactamente lo que se quiere probar, sí no se está claro cómo se prueba, o si el análisis del resultado se hace a simple vista. Estas mismas ideas se suelen agrupar diciendo que un caso de prueba consta de 3 bloques de información:

- El propósito de la prueba.
- Los pasos de ejecución de la prueba.
- El resultado que se espera.

Todos y cada uno de esos puntos deben quedar perfectamente documentados. El plan de pruebas señala el enfoque, los recursos y el

esquema de actividades de prueba, así como los elementos a probar, las características, las actividades de prueba, el personal responsable y los riesgos. Una estrategia de prueba propone movernos hacia afuera en una espiral, de manera que primero se prueban las unidades más pequeñas del diseño del software (clases o módulos) y después como se integran los componentes en los cuales están contenidas estas unidades. A partir de un caso de uso se pueden realizar pruebas de caja negra, obteniéndose varios casos de prueba que permiten:

- Verificar el resultado de la interacción entre los actores y el sistema.
- Comprobar que se satisfagan las pre-condiciones y post-condiciones del caso de uso.
- Comprobar que se siga la secuencia de acciones especificado por el caso de uso.

		Código:	**H01**
Tipo de Documento:	**Caso de Prueba**	**Pág. 1 de 1**	
Propósito: Determinar la existencia de validaciones en la entrada de datos para la creación de empleados en el Sistema de Control de Acceso de Personal.			
Tipo de Prueba	Caja Negra – Cumplimiento de Requisitos		
Auditor:		Fecha	
Empresa:			
Preguntas			
Prerrequisitos:	1. Tener instalado el Sistema de Control de Acceso de Personal. 2. Poseer un usuario con privilegios para acceder al sistema y al módulo de definición de empleados.		
Pasos:	1. Ingresar al módulo administrativo del sistema de Control de Acceso de Personal. 2. Ingresar al menú de **Definiciones** y seleccionar la opción **Empleados**. 3. En el formulario de Empleados presionar el botón **Nuevo**. 4. Verificar que se habiliten todos los campos para su edición. 5. Presionar el botón **OK** sin ingresar ninguna información y verificar que se valide a nivel de aplicación a través de un mensaje al usuario, la inserción de datos obligatorios, como cédula, nombre, Tipo de Usuario y contraseña. 6. Ingresar los datos obligatorios para la creación de un cliente. 7. Presionar el botón **OK** nuevamente. 8. Presionar el botón salir para cerrar el formulario. 9. Ingresar nuevamente al menú de **Definiciones** y seleccionar la opción **Empleados**. 10. Posteriormente, presionar el botón **Buscar**. 11. Constatar que el usuario que se creó aparece en la lista de usuarios registrados en el sistema. 12. Presionar el botón **Salir** hasta salir de la aplicación.		
Resultados Esperados:	1. Mensajes de validación de ingreso de datos en el formulario. 2. Usuario registrado en la base de datos del sistema.		
Observaciones:	_____ _____ _____ _____		

Cuadro 13. Ejemplo: Caso de Prueba, Caja Negra.

Al realizar este tipo de auditoría, el estudiante debe dejar muy claro a la organización que no va a revisar la información que se encuentra en las bases de datos, sino que simplemente va a analizar el rendimiento de las mismas para garantizar la integridad, confidencialidad y disponibilidad de los datos, en otras palabras, no se evalúa el contenido de los datos sino la configuración y el funcionamiento del gestor de bases de datos que la organización utiliza.

Para realizar esta evaluación, el auditor puede valerse de importantes herramientas de software como es el caso de DB Audit y utilizar los resultados que arroja como papeles de trabajo.

Aunque existen distintas metodologías que se aplican en auditoría informática de bases de datos (prácticamente cada firma de auditores y cada empresa desarrolla la suya propia), se pueden agrupar en 2 clases.

METODOLOGÍA TRADICIONAL

En este tipo de metodología el auditor revisa el entorno con la ayuda de una lista de control (check list) que consta de una serie de cuestiones a verificar (Ver Anexo D). El auditor deberá registrar el resultado de su investigación. Este tipo de técnica suele ser aplicada a la auditoría de bases de datos, especificándose en la lista de control todos los aspectos a tener en cuenta. Así por ejemplo, si el auditor se enfrenta a un entorno Oracle, en la lista de control se recogerán los parámetros de instalación que más riesgos comportan, señalando cuál es su rango adecuado. De esta manera si el auditor no cuenta con la asistencia de un experto en el producto, puede comprobar por lo menos los aspectos más importantes de su instalación.

Este tipo de metodología, conocida también como **risk oriented approach**, es la que propone ISACA y empieza fijándonos objetivos de control que minimizan los riesgos potenciales a los que está sometido el entorno. Una vez establecidos los objetivos de control, se especifican las técnicas específicas correspondientes a dichos objetivos. Un objetivo de control puede llevar asociadas varias técnicas que permiten cubrirlo en su totalidad. Estas técnicas pueden ser preventivas (controlar acceso a la BD), detectivas (monitorizar accesos a la BD) o correctivas (copias de respaldo).

En caso de que los controles existan, se diseñan unas pruebas (denominadas pruebas de cumplimiento) para verificar la consistencia de los mismos. Si estas pruebas detectan inconsistencias en los controles, o bien, si los controles no existen, se pasa a detectar otro tipo de pruebas (denominadas pruebas sustantivas) que permitan dimensionar el impacto de estas deficiencias. A continuación se describe un breve ejemplo:

Objetivo de control: El Sistema de Gestión de Bases de Datos (SGBD) deberá preservar la confiabilidad de la base de datos.

Técnicas de control: Se deberán establecer los tipos de usuarios, perfiles y privilegios necesarios para controlar el acceso a la base de datos.

Prueba de cumplimiento: Listar los privilegios y perfiles existentes en el SGBD.

Prueba sustantiva: Comprobar si la información ha sido corrompida comparándola con otra fuente, o revisando los documentos de entrada de datos y las transacciones que se han ejecutado.

Los procesos de desarrollo de software también pueden ser auditados, para que el auditor pueda ser capaz de lograr esto, debe tener amplios conocimientos sobre metodologías de desarrollo de software, las fases que las componen y los respectivos entregables (también llamados artefactos) que se generan en cada una de estas fases. Recuerde que no se puede evaluar algo sin tener previamente el conocimiento adecuado.

Algunas organizaciones que desarrollan software establecen sus propias metodologías de desarrollo y en estos casos, el auditor debe documentarse en los procesos que la organización lleva a cabo. En el caso de que la metodología exista, pero no esté documentada por la organización, el auditor deberá documentarla para establecer un marco de referencia y realizar la comparación con la realidad de la organización. Sólo de esta manera, el auditor podrá determinar si en la organización se realizan los procedimientos como corresponden.

Durante los procesos de desarrollo de software se realizan las llamadas **pruebas de caja blanca** (también conocidas como pruebas de caja de cristal o pruebas estructurales) que se centran en los detalles procedimentales del software, por lo que su diseño está fuertemente ligado al código fuente. El probador escoge distintos valores de entrada para examinar cada uno de los posibles flujos de ejecución del programa y cerciorarse de que se devuelven los valores de salida adecuados.

Aunque las pruebas de caja blanca son aplicables a varios niveles —unidad, integración y sistema—, habitualmente se aplican a las unidades de software. Su cometido es comprobar los flujos de ejecución dentro de cada unidad (función, clase, módulo, etc.) pero también pueden probar los

flujos entre unidades durante la integración, e incluso entre subsistemas, durante las pruebas de sistema.

Durante las auditorías de desarrollo de software, el principal objetivo es evaluar si el proceso se realiza coherentemente y si los entregables son adecuados, sin embargo, es importante que el auditor tenga conocimiento sobre las pruebas de caja blanca y de esta manera pueda evaluar si el equipo desarrollador las está realizando bien. Las principales técnicas de diseño de pruebas de caja blanca son:

- Pruebas de flujo de control.
- Pruebas de flujo de datos.
- Pruebas de bifurcación (branch testing).
- Pruebas de caminos básicos.

Se invita al lector a investigar sobre estos tipos de pruebas y de así ampliar sus conocimientos en esta materia.

AUDITORÍA INFORMÁTICA DE SEGURIDAD

Este tipo de auditoría puede complementarse muy bien con otras ya que principalmente se orienta a verificar las políticas de seguridad de la información de la organización. Una política de seguridad de la información es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información en una entidad, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.

El cumplimiento de las políticas y estándares de seguridad de la información es obligatorio y debe ser considerado como una condición en los contratos del personal. En las políticas se definen los roles y

responsabilidades a lo largo de la organización con respecto a la protección de los recursos de información.

En este tipo de auditoría se evalúan básicamente dos tipos de seguridad: seguridad física y seguridad ligada al personal, sin embargo, como se mencionó anteriormente se pueden crear tipos de auditorías mixtas, por ejemplo: auditoría de seguridad de redes. En esta auditoría se podría evaluar la seguridad física de los recursos que componen la red y también la seguridad ligada al personal que tiene acceso a la red.

En este tipo de auditoría es importante considerar los siguientes aspectos:

- Análisis de Riesgos.
- Outsourcing (contratación de terceros).
- Clasificación del acceso a la información.
- Aplicación de controles.
- Seguridad del personal.
- Información almacenada en medios digitales o físicos.

SEGURIDAD FÍSICA

Dentro de la seguridad física deben considerarse los Requisitos de las localizaciones y edificios. Algunos de los aspectos más importantes a evaluar tanto en para la auditoría como para el análisis de riesgos son:

- Protección de las personas y de los elementos que componen un sistema de información.
- Gestionar acceso físico a las instalaciones.
- Factores ambientales.

Los recursos para el tratamiento de la información crítica o sensible para la Organización deben ubicarse en áreas seguras, protegidas por un perímetro de seguridad definido, con barreras de seguridad y controles de entrada apropiados.

Algunos de los controles a considerar son:

- **Perímetros de seguridad física:** Perímetro de seguridad definidos, muros sólidos, mecanismos de control de acceso físico al lugar, alarmas.
- **Controles físicos de entrada:** Controles físicos de entradas, controles de acceso al personal, revisión de derechos de accesos.
- **El trabajo en áreas seguras:** Trabajo en áreas seguras, supervisión en las áreas, monitorear visitas de terceros, evitar equipos de videos, fotografías y audio.
- **Mantenimiento de equipos:** Mantenimiento de equipos, cumplir con el mantenimiento, registro de fallos, medida para el envío de los equipos fuera de las instalaciones.
- **Seguridad en la reutilización o eliminación de equipos:** Seguridad en la reutilización y eliminación de equipos, destrucción física de manera segura, comprobación de que el dato sensible ha sido borrado.
- **Política de puesto de trabajo despejado y bloqueo de pantalla.**

SEGURIDAD LIGADA AL PERSONAL

Dentro de la seguridad ligada al personal no solo se supervisan los permisos que poseen los usuarios para acceder a los medios informáticos, adicionalmente deben considerarse las políticas y procedimientos que tiene la organización para la incorporación o desincorporación de personal a su plantilla (con los cambios a nivel de roles y perfiles que corresponden).

Algunos de las áreas que pueden ser evaluadas son:

Seguridad en la definición de trabajo y los recursos inclusión de seguridad en las responsabilidades laborales: Las funciones y responsabilidades sobre la seguridad de la información, deberían documentarse cuando sea apropiado. Deberían incluir toda responsabilidad general para implantar o mantener la política de seguridad, así como cualquier responsabilidad específica para la protección de activos particulares y la ejecución de procesos o actividades particulares de seguridad.

Selección y política del personal: Deberían realizarse comprobaciones en la plantilla fija en el momento de la solicitud de trabajo. Esto debería incluir controles como los siguientes:

- La disponibilidad de referencias satisfactorias sobre actitudes, por ejemplo, una personal y otra de la Organización.
- La comprobación (de la completitud y precisión) del Curriculum Vitae del candidato.
- La confirmación de las certificaciones académicas y profesionales.
- Una comprobación independiente de la identificación (con pasaporte o documento similar).

Acuerdos de confidencialidad: Se usan acuerdos de confidencialidad o no divulgación para notificar qué información es secreta o confidencial. Los empleados normalmente deberían firmar dicha cláusula como parte de sus términos o condiciones iniciales de trabajo. La Organización debería requerir la firma de un acuerdo de confidencialidad a los recursos humanos externos o los usuarios de terceros no cubiertos por un contrato de trabajo (que contiene cláusulas de confidencialidad) antes de su acceso a los recursos de tratamiento de información.

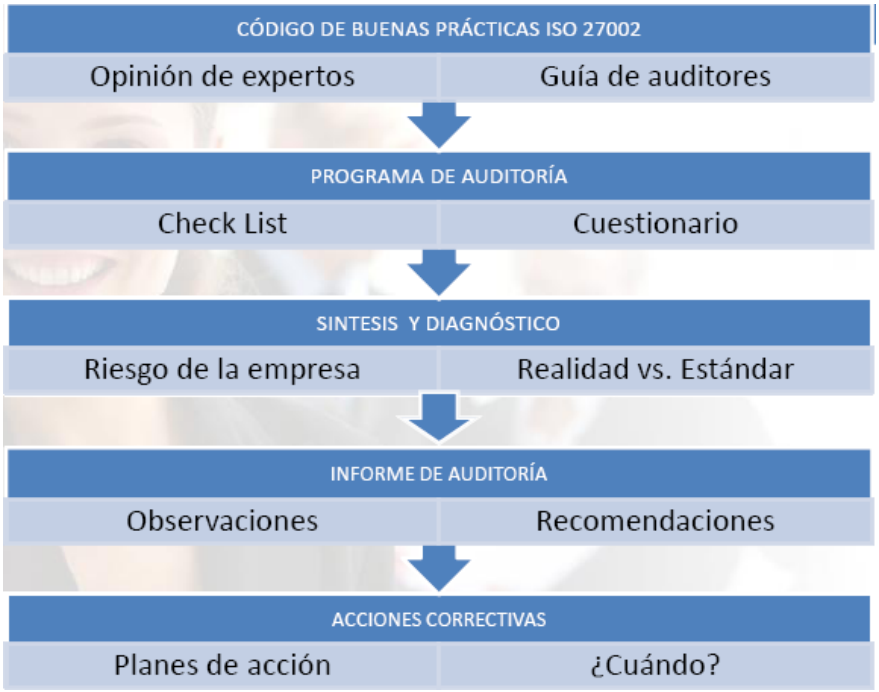


Figura 30. Resumen Auditoría de Seguridad.

AUDITORÍA INFORMÁTICA DE REDES

La auditoría de red es una de las más amplias, ya que pueden evaluarse varios aspectos de las redes, según se hayan contemplado dentro del alcance de la auditoría.

Es de gran importancia destacar la definición y establecimiento de los puntos que se deben evaluar, como elemento fundamental de apoyo al auditor, debido a que esto es producto de un análisis previo, tanto del origen de la auditoria y de la definición previa de los objetivos que se pretenden satisfacer con la realización de la auditoria de red.

Para realizar este tipo de auditoría, el auditor puede apoyarse en herramientas de software que le permitan realizar las pruebas correspondientes a cada área de la red que se estudia.

ÁREAS A EVALUAR

Figura 31. Áreas a Evaluar en Auditoría de Red.

A continuación se describen las diferentes áreas a evaluar de la red, adicionalmente se identifican las sub-áreas y los aspectos que pueden ser auditados.

OBJETIVOS

Sub-Áreas	Aspectos a Auditar
Uso de metodología	Controles en: normas, estándares y políticas para el análisis y diseño.
Cumplimiento de objetivos para instalar la red	Compartir los recursos informáticos.

	Disponibilidad y cobertura de los servicios de comunicación e informáticos. Integridad, confiabilidad, información institucional. Satisfacción necesidades del poder computacional.
Delimitación de la Red	Temporal: Tiempo en que se instala o rediseña la red. Espacial: Dimensiones lógicas y físicas. Conceptual: Análisis de las necesidades que deben cumplir la red. Tecnológica: Requerimientos y conocimientos Informáticos.
Viabilidad y Factibilidad del diseño e instalación	Tecnológica. Económica. Administrativa. Operativa.
Diseño e implementación cobertura de la Red	Análisis Red LAN, WAN, MAN, Redes Públicas e Inalámbricas. Evaluar el uso adecuado y confiable de la tecnología para transmitir datos. Restricciones para el tamaño de la red. Evaluar tiempo promedio de transmisión de la red. Evaluar las velocidades para la transmisión

Sub-Áreas	Aspectos a Auditar
Análisis funcionamiento y confiabilidad dispositivos de Red	Repetidores: Ampliar las señales Puentes: Guardan y renvían los datos en la red. Nivel de enlace. Enrutadores de protocolos múltiples: Son como puentes y permiten la conexión de redes diferentes protocolos. Gateway: Permiten la conexión de las redes en el nivel de transporte.
Diseño e implementación cobertura de la Red	Análisis Red LAN, WAN, MAN, Rede Públicas e Inalámbricas. Evaluar el uso adecuado y confiable de la tecnología para transmitir datos. Restricciones para el tamaño de la red. Evaluar tiempo promedio de transmisión de la red. Evaluar las velocidades para la transmisión. Puertas de enlace de aplicación: Conectan dos partes de una aplicación, aunque éstas utilicen formatos distintos.
Análisis del diseño e implementación Servidores	Características y componentes: marca, modelo y serial.

	Servidor principal dedicado y no dedicado. De Archivos. De Impresión. De Comunicación Gateway: Permiten la conexión de las redes en el nivel de transporte.
Análisis del diseño e implementación estaciones de trabajo	Características y componentes: marca, modelo y serial. Número de estaciones de trabajo. Tarjeta de interfaz de red.

COMPONENTES LÓGICOS

Sub-Áreas	Aspectos a Auditar
Análisis uso y funcionamiento adecuado del software de red	Sistemas Operativos para el funcionamiento red. Lenguajes y programas de desarrollo de la red. Programas y paquetes de aplicación de la red. Utilerías, librerías y bibliotecas de red. Disponibilidad de licencias y permisos de instalación del software de red. Actualización informática y de los proveedores de sistemas de la red. Actualización tecnológica del software desarrollado por la organización y del mercado.

	Administración y Control de utilerías, librerías, bibliotecas de red, juegos y aplicaciones no autorizadas. Bitácoras de los accesos de los usuarios.

ELEMENTOS DE LA RED

Sub-Áreas	Aspectos a Auditar
Análisis instalación física de la red	Diseño arquitectónico de las instalaciones (toma corriente).
Análisis funcionamiento de los medios de transmisión físico	Cableado y conectores. Transmisión por radio, microondas, satelital, infrarrojo. Combinación entre ambos medios de transmisión.
Análisis de los técnicas de los medios físicos de transmisión	Síncrona Asíncrona Analógica Digital Serie Paralelo

CONECTIVIDAD

Sub-Áreas	Aspectos a Auditar
Análisis funcionamiento del modelo OSI (Modelo de Referencia de Interconexión de Sistemas Abiertos)	Nivel Físico: Establecimiento de una conexión por un medio físico (coaxial, fibra, línea telefónica, satélite…).

	Enlace: Controla la transferencia de datos, detecta y corrige los errores de bits que se producen en la ruta. Garantiza la transferencia segura de las tramas al destino. Red: El ruteo de los paquetes desde su fuente a su destino. Proporciona medios para establecer, mantener y liberar las comunicaciones entre sistemas finales. Transporte: Nivel de comunicación directa de su par en el destino, controla la transferencia entre sistemas abiertos terminales. Sesión: proporciona los medios necesarios para que las entidades de presentación organicen y sincronice el dialogo y procedan al intercambio de datos. Presentación: Permite la representación de la información. Aplicación: Contienen todas las funciones que implican una comunicación con sistemas abiertos (ejemplo: correo electrónico). Evaluar el tiempo promedio.
Análisis servicios red (transferencia voz, datos y audio)	Funcionamiento de las terminales para la conexión o no conexión.

	Adecuado funcionamiento de los protocolos. Velocidad de la transmisión de datos en la red. Administración y control de la seguridad de la red. Funcionamiento del nivel de Internet. Control del tráfico de la red. Control de la congestión en el nivel IP. Evaluar el funcionamiento del FTP, SMTP, SNMP. Evaluar el tiempo promedio de transmisión de la red. Funcionamiento de las técnicas de transferencia de datos: Simplex (1 sólo sentido), Half-duplex (En 2 sentido, pero uno a la vez) y full-duplex (ambos sentidos a la vez) Disponibilidad y cobertura de los servicios de comunicación e informáticos. Integridad, confiabilidad, información institucional. Satisfacción necesidades del poder computacional.

PROTOCOLOS DE COMUNICACIÓN

Sub-Áreas	Aspectos a Auditar
Análisis funcionamiento de los Protocolos	IP: Protocolo Internet. ICPM: Protocolo de Mensajes de Control de Internet. TCP: Protocolo de Control de Transmisión. UDP: Protocolos de Datagrama de Usuario. FTP: Protocolo de Control de Transferencia. SMTP: Protocolo Simple de Transporte de Correo. SNTP: Protocolo Simple de Administración de Red. DNS: Sistema de Nombres de Dominio. Telnet: Red de Telecomunicaciones.

TOPOLOGÍA

Sub-Áreas	Aspectos a Auditar
Análisis de los tipos de topología usados en la red	Necesidades de cobertura de la topología física y lógica de la red. Evaluación del diseño e instalación de la red según su configuración: punto a punto, cliente/servidor, multipuntos, conexión inalámbrica, conexión virtual.

	Tipos de topología: Bus, Estrella, Anillo, Malla y Doble anillo.

ADMINISTRACIÓN DE RED

Sub-Áreas	Aspectos a Auditar
Actividades a Evaluar	Análisis del acceso información institucional, privilegios y niveles de operación de los datos, a los sistemas y software. Análisis del cambio periódico de los niveles, privilegios y contraseñas. Análisis de los reportes de incidencias y circunstancias que afecten el funcionamiento de la red, a su información o software. Análisis de la atención y rapidez de respuesta para satisfacer las necesidades informáticas. Análisis de la existencia, acatamiento y actualización de las políticas y reglamentos del uso del sistema de red. Análisis del cumplimiento de la actividad informática de los servidores, estaciones, sistemas y componentes de red. Análisis operación de la red. Análisis del control de flujo y velocidad de transmisión de datos en la red.

	Análisis de los reportes y estadísticas periódicas de la auditoria de la red. Análisis administración y control de alta disponibilidad y redundancia de la red.

SEGURIDAD DE RED

Sub-Áreas	Aspectos a Auditar
Incidencias	Caída del sistema y enlaces. Pérdida de Información. Sabotaje en la Red. Colisiones. Filtraje de la información. Violación de políticas de seguridad de la red. Fallas en los equipos. Violación de email y contraseñas. Desactualizaciones sistemas de protección a la redes. Deficiente tráfico de la red. Destrucción de soportes documentales. Agujeros de seguridad en redes conectadas. Virus.
Controles Estándar ISO 27033-1	Alerta. Arquitectura. Ataques. Auditando login.

	Herramientas de Auditoria. Certificación de autorización. Política corporativa de protección de la información. Zona desmilitarizada. Negación de servicios. Extranet. Filtrado. Cortafuegos. Hub.
Identificando Riesgos y preparándose para identificar los controles	Información en corriente y/o planificando la red. La Protección de la Información a riesgos y áreas potenciales de control.
Soporte de controles	Gerencia de seguridad de red. Background.
Protección contra riesgos	Almacenamiento información Actos ilegales: Sabotajes, extorsión, alteración, destrucción o fraudes. Mal uso de la información: invasión privacidad, mal uso de la confiabilidad, uso inadecuado de los datos. Piratería y robo de información. Alto índice de incidencias en la red. Actos no intencionales: negligencia, descuido, fallas del equipo y del sistema, fallas externas.

	Actos no intencionales: negligencia, descuido, fallas del equipo y del sistema, fallas externas virus informáticos.

NOTAS DEL LECTOR

El lector puede aprovechar este espacio para escribir algunas notas relacionadas con los tópicos estudiados en este capítulo.

CAPÍTULO V

FASE III: ELABORACIÓN DEL PRE-INFORME E INFORME FINAL

Luego de un largo y minucioso proceso de auditoría, el cual ha sido ilustrado en los capítulos anteriores, hemos llegado a la última etapa. Todas las técnicas utilizadas al realizar la auditoría tendrán como fruto un informe que recoge los resultados obtenidos. Este producto será el que se mostrará a los directivos de la organización, quienes no necesariamente corresponden al área tecnológica (gerentes, administradores, contadores, entre otros) y por lo cual debe ser fácil de entender.

Lograr esta simpleza al momento de comunicar los resultados no es sencillo después de haber recopilado tantos datos y de haber realizado diversas pruebas, por ello la importancia de que el informe sea preciso. Para que se visualice de manera más didáctica, consideramos necesario dividir esta tercera fase en dos partes.

PRE-INFORME

Esta primera parte corresponde a la fase de síntesis y diagnóstico de la auditoría, donde el auditor o equipo de auditores procesa todos los datos y observaciones recopilados durante la ejecución de la auditoría.

NOTA: Es importante comentar que esta etapa de elaborar el pre-informe se podría incluir en un trabajo especial de grado como un procedimiento de la investigación, donde se incluyan las pruebas realizadas, los resultados de dichas pruebas y las evidencias recolectadas. Posteriormente, se recomendaría que el informe final, por ser un producto breve y sintetizado, sea incluido como un anexo dado su calidad de entregable.

EVIDENCIA DE AUDITORÍA

Según el diccionario de la Real Academia Española, se define el concepto de **Evidencia** como una prueba determinante en un proceso. En la auditoría, toda la evidencia se recolecta durante la fase de ejecución para posteriormente ser analizada y elaborar un informe previo, el cual luego puede ser depurado y adaptado al formato ideal para su entrega. La obtención, manipulación y resguardo de la evidencia es sumamente importante ya que el auditor accede en muchos casos a información sensible de la organización, y en base a la misma, se logrará realizar un diagnóstico real del área de la organización auditada. ISACA, dentro de sus estándares, contempla algunas normativas relacionadas con la evidencia.

El auditor debe aplicar procedimientos de prueba adicionales para lograr una evidencia de auditoría suficiente y apropiada en circunstancias en las que el trabajo de otros expertos no la proporciona. Durante el transcurso de la auditoría, el auditor debe obtener evidencia suficiente, confiable y pertinente para alcanzar los objetivos de auditoría. Los hallazgos y conclusiones de la auditoría deberán ser soportados mediante un apropiado análisis e interpretación de dicha evidencia. El proceso de auditoría deberá documentarse, describiendo las labores de auditoría realizadas y la evidencia de auditoría que respalda los hallazgos y conclusiones del auditor.

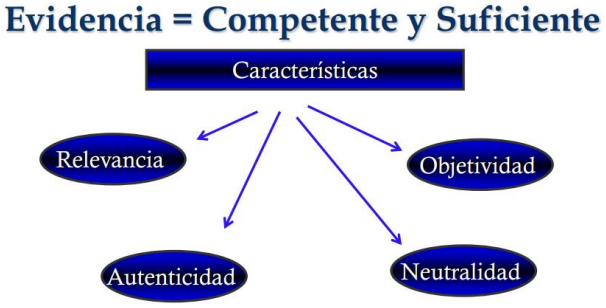


Figura 32. Características de la evidencia de auditoría.

Algunos factores que afectan la obtención de evidencia son:

- Nivel del riesgo inherente.
- Evaluación de riesgos de control.
- Volumen de transacciones a examinar.
- Experiencia del auditor.
- Origen y confiabilidad de la información disponible.

Figura 33. Tipos de evidencia de auditoría.

Algunos de los estándares de ISACA con respecto a la evidencia son:

El auditor debe obtener evidencias de auditoría suficientes y apropiadas para llegar a conclusiones razonables sobre las que basar los resultados de la auditoría.

El auditor debe evaluar la suficiencia de las evidencias de auditoría obtenidas durante la misma.

EVIDENCIA APROPIADA

Evidencia de auditoría:

- Incluye los procedimientos realizados por el auditor.

- Incluye los resultados de los procedimientos realizados por el auditor.
- Incluye los documentos fuente (en formato electrónico o impresos en papel), registros e información de corroboración utilizados para apoyar la auditoría.
- Incluye los hallazgos y resultados del trabajo de auditoría.
- Demuestra que el trabajo fue realizado y cumple con las leyes, normativas y políticas aplicables.

Al obtener una evidencia de auditoría de una prueba de controles, el auditor debe considerar la completitud de la evidencia de auditoría para apoyar el nivel de riesgo del control evaluado.

Es necesario identificar, obtener las referencias cruzadas y catalogar de forma adecuada la evidencia de auditoría.

Deben tenerse en cuenta propiedades tales como la fuente, naturaleza (por ejemplo, escrito, oral, visual, electrónica) y autenticidad (por ejemplo, firmas digitales y manuales, sellos) de la evidencia de auditoría al evaluar su nivel de fiabilidad.

EVIDENCIA FIABLE

En términos generales, la fiabilidad de la evidencia de auditoría es mayor cuando:

- Aparece en forma escrita, en lugar de presentarse como expresiones orales.
- Se obtiene de fuentes independientes.
- Es obtenida por el auditor en lugar de obtenerlo de la entidad que se está auditando.
- Es certificada por una entidad independiente.

- Es mantenida por una entidad independiente.

El auditor debe considerar la forma más económica de recopilar la evidencia necesaria para satisfacer los objetivos y riesgos de la auditoría. Sin embargo, la dificultad o coste no es una razón válida para omitir un proceso necesario.

Los procedimientos usados para recopilar evidencias de auditoría dependen de la temática auditada (es decir, su naturaleza, plazos de la auditoría, juicio profesional). El auditor debe seleccionar el procedimiento más apropiado para cada objetivo de auditoría.

El auditor puede obtener una evidencia de auditoría por:

- Inspección.
- Observación.
- Consulta y confirmación.
- Repetición de la ejecución.
- Repetición del cálculo.
- Computación.
- Procedimientos analíticos.
- Otros métodos generalmente aceptados.

El auditor debe considerar la fuente y la naturaleza de cualquier información obtenida para evaluar su fiabilidad y ulteriores requisitos de verificación.

EVIDENCIA SUFICIENTE

La evidencia puede considerarse suficiente si soporta todas las preguntas materiales referentes al objetivo y al alcance de la auditoría.

La evidencia de auditoría debe ser objetiva y suficiente para permitir que un tercero independiente repita la ejecución de las pruebas y obtenga los mismos resultados. La evidencia debe ser proporcional a la materialidad del elemento y a los riesgos involucrados.

La suficiencia es una medida de la cantidad de evidencias de auditoría, mientras que lo apropiado es la medida de la calidad de la evidencia de auditoría, estando ambos conceptos relacionados entre sí.

En este contexto, cuando se obtiene información de la organización que es utilizada por el auditor para realizar los procedimientos de auditoría, el auditor debe también poner énfasis en la precisión y completitud de la información.

En aquellas situaciones en las que el auditor cree que no se puede obtener evidencia suficiente de auditoría, el auditor deberá reportar este hecho de una manera coherente durante la comunicación de los resultados de auditoría.

PROTECCIÓN Y RETENCIÓN

La evidencia de auditoría debe protegerse de accesos y modificaciones no autorizados.

La evidencia de auditoría debe retenerse después de completarse el trabajo de auditoría durante el tiempo que resulte necesario para cumplir con todas las leyes, normas y políticas aplicables.

INFORME FINAL

Después de haber analizado y sintetizado toda la información y evidencia obtenida, llegamos a la segunda parte, donde el auditor debe suministrar un informe, en un formato apropiado, al finalizar la auditoría.

El informe debe identificar la organización, los destinatarios previstos y respetar cualquier restricción con respecto a su circulación. Además debe indicar el alcance, los objetivos, el período de cobertura y la naturaleza, plazo y extensión de las labores de auditoría realizadas.

El informe debe indicar los hallazgos, conclusiones y recomendaciones, así como cualquier reserva, calificación o limitación que el auditor tuviese en cuanto al alcance de la auditoría.

Para que el informe tenga credibilidad, el auditor debe tener evidencia de auditoría suficiente y apropiada para respaldar los resultados reportados.

Al emitirse, el informe del auditor debe ser firmado, fechado y distribuido de acuerdo con los acuerdos previos entre el auditor y la organización. En la vida real, suelen elaborarse contratos de auditoría o cartas de compromiso y en base a sus términos se establece el alcance, objetivos y los involucrados en el proceso de auditoría.

El auditor debe, donde resulte apropiado, considerar el uso del trabajo de otros expertos para realizar la auditoría. El auditor debe evaluar y estar satisfecho con las credenciales profesionales, competencias, experiencia relevante, recursos, independencia y procesos de control de calidad de otros expertos, antes de su contratación.

El auditor debe evaluar, revisar y calificar el trabajo de otros expertos como parte de la auditoría y concluir el grado de utilidad y la fiabilidad del trabajo del experto. El auditor debe determinar y concluir si el trabajo de otros expertos resulta adecuado y suficiente para permitir que el auditor saque sus conclusiones con respecto a los objetivos actuales de la auditoría. Dicha conclusión debe documentarse claramente. En todos los casos, el auditor es el responsable de que otros expertos contratados por él, no usen indebidamente las evidencias recolectadas.

El informe debe incluir dentro de sus características:

- Claridad
- Confiabilidad
- Propiedad
- Concisión
- Sencillez
- Asertividad
- Ilación
- Tono y fuerza
- Oportunidad
- Precisión
- Exactitud
- Imparcialidad
- Objetividad
- Congruencia
- Veracidad
- Efectividad
- Sintaxis

HALLAZGOS DE AUDITORÍA

Los hallazgos contemplan las observaciones que hemos realizado durante la etapa de ejecución de la auditoría y también durante el diagnóstico. No solamente incluyen las cosas que están marchando mal en la organización, sino que pueden incluirse también las cosas que aunque

se están cumpliendo, deben ser mejoradas. Los hallazgos son redactados en forma concreta por tanto son hechos determinados por las evidencias obtenidas.

Ejemplo: Archivos de la base de datos no cifrados.

CONCLUSIONES

Luego de establecer los hallazgos, se pueden elaborar las conclusiones. Son redactadas en forma profesional (con conocimiento suficiente en la materia) y de alguna manera hacen referencia a los hallazgos, pero resaltan la importancia de que la organización los tome en cuenta.

Ejemplo: Es importante para la organización que la información de su base de datos se encuentre cifrada (codificada), de esta manera, si llegasen a ser obtenidas por individuos no autorizados, se evitaría o dificultaría que los mismos pudiesen acceder a cualquier tipo de información sensible que contenga la misma y que podría poner en riesgo los objetivos del negocio.

OPINIÓN DEL AUDITOR

El auditor debe proporcionar una opinión de auditoría apropiada e incluir los límites del alcance cuando no se obtenga la evidencia requerida mediante procedimientos de prueba adicionales. El auditor como experto puede brindar un **Dictamen** donde se refleje el estado real del área auditada. Puede ser **Favorable** (con o sin salvedades), **Adverso**, **Abstenerse** de dar una opinión o presentar una **Opinión Parcial** en base a la poca evidencia obtenida.

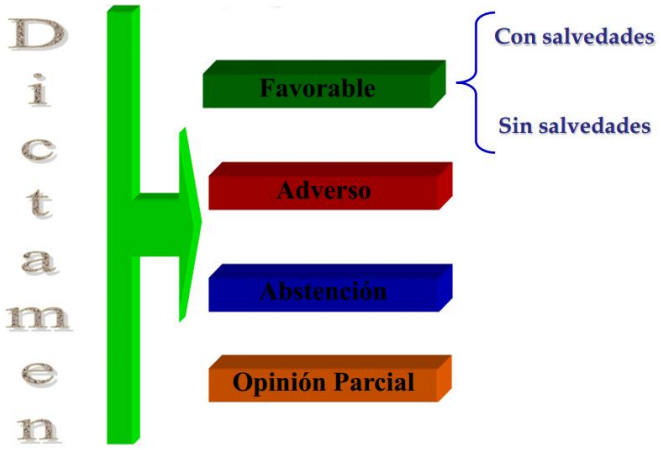


Figura 34. Dictamen de auditoría.

RECOMENDACIONES

Posterior al proceso de detectar las fallas y reflejar la importancia de solucionarlas, es necesario que el auditor proporcione a la organización las recomendaciones pertinentes para solventar estos problemas. Las recomendaciones se redactan de forma tal que se haga una recomendación profesional y viable, identificándola, pero sin expresar la solución. Al referirnos a que la recomendación sea viable, nos referimos a que se adapte a las condiciones (presupuesto, personal, espacio físico, entre otras) de la empresa. También es importante que en cada recomendación se identifique la persona, cargo o departamento a la que está dirigida, de esta manera pueden establecerse compromisos y lapsos de tiempo para que sean tomadas en cuenta. Como se mencionó anteriormente, se recomienda lo que se debe hacer, pero no la forma en que se debe hacer ni los paquetes de software que podrían utilizarse. Resolver la problemática sería un nuevo servicio que usted como consultor puede ofrecerle a la organización.

Ejemplo: Se recomienda al Gerente de Sistemas, establecer un mecanismo o procedimiento de cifrado de la base de datos en un lapso no mayor de tres (03) meses.

ESTRUCTURA DEL INFORME

La estructura del informe puede variar según el auditor o grupo de auditores, sin embargo, existen algunos requisitos considerados mínimos que debe contemplar. A continuación se plantea una estructura básica que contempla todos estos aspectos:

1. **Identificación del informe:** Identifique el tipo de auditoría informática que está realizando, es conveniente colocarle nuestro logo para darle mayor presencia.
2. **Histórico de revisiones:** Se incluye un registro de versiones y fechas de modificaciones. Cuando nuestra auditoría es la primera, suele identificarse con la versión 0.
3. **Índice:** Una tabla de contenidos donde se muestren los aspectos contemplados en el informe final.
4. **Introducción:** Un breve texto donde se exprese la importancia de la auditoría informática y sus ventajas.
5. **Identificación de la Entidad Auditada:** Nombre de la Empresa Auditada.
6. **Identificación del Cliente:** Indique de ser el caso el área (Dpto., unidad, etc.) de la empresa auditada.
7. **Alcance de la Auditoría:** Se incluye el alcance desarrollado en la planificación de la auditoría.
8. **Objetivos:** Se incluyen los objetivos generales y específicos determinados en la planificación de la auditoría.
9. **Hallazgos de Auditoría**.
10. **Conclusiones**.
11. **Recomendaciones**.
12. **Dictamen de Auditoría:** Este apartado no es obligatorio (según sea el caso).
13. **Fecha del Informe**.

14. **Identificación y Firma del Auditor**.

	Planificación	Ejecución	Informe
Fechas	xx/xx/xx al xx/xx/xx	xx/xx/xx al xx/xx/xx	xx/xx/xx al xx/xx/xx

Apellidos y Nombres	Cargo	Firma
Juan Pérez	Auditor Sénior	

Figura 35. Identificación y firma del auditor.

El lector podrá encontrar un informe final de auditoría en el Anexo B. Este informe es de carácter ilustrativo y sirve como ejemplo de la estructura básica que debe poseer un informe final de auditoría. La organización que está siendo evaluada y la firma de consultores que realiza la auditoría son ficticias, sin embargo, los resultados obtenidos son similares a los que se podría encontrar un auditor en un caso real.

REFERENCIAS

Camacaro, M. Castillo, L. Díaz, A. Matute, L. Mujica M. y Sierralta, M. (2013). *Diplomado de Auditoría Informática*. Barquisimeto, Venezuela: Universidad Centroccidental "Lisandro Alvarado".

Camacaro, M. (2009). *Modelo de Gerencia Estratégica del Conocimiento para las Universidades Públicas. Caso: Universidad Centroccidental "Lisandro Alvarado". Periodo 1997-2008*. Tesis Doctoral, Universidad Santa María. Caracas, Venezuela.

Castellanos, L. (2009). *PERT-CPM: una guía práctica y sencilla*. Maracaibo, Venezuela.

Chiavenato, Idalberto. (2006). *El Proyecto de Investigación: Introducción a la metodología científica*. Caracas, Venezuela: McGraw-Hill Interamericana.

Hernández Sampieri, R. Fernández Collado, C. y Baptista Lucio, P. (1991). *Metodología de la Investigación*. Mexico: Mc Graw-Hill.

Colaboradores de Ecured.cu (sf). *Ecured.cu* [Documento en línea]. Disponible: http://www.ecured.cu/index.php/Pruebas_de_caja_negra. [Consulta: 2014 agosto 28].

Colaboradores de Tuguiacontable.org (sf). *Tuguiacontable.org* [Documento en línea]. Disponible: http://www.tuguiacontable.org/app/article.aspx?id=119. [Consulta: 2014 agosto 14].

González, R. y Jimeno, J. (2012). *Check list / Listas de chequeo: ¿Qué es un checklist y cómo usarlo?* [Documento en línea]. Disponible: http://www.pdcahome.com/check-list/. [Consulta: 2014 agosto 27].

Instituto Universitario Politécnico “Santiago Mariño” (2006). *Manual de Trabajo de Grado*. Caracas, Venezuela.

ISACA (2012). *Glosario de Términos Inglés-Español*.

ISO/IEC 27001:2005. *Information technology - Security techniques – Information security management systems - Requirements*.

ISO/IEC 27005:2008. *Information technology -- Security techniques -- Information security risk management*.

ISO/IEC Guía 73:2002. Risk management -- Vocabulary -- Guidelines for use in standards.

Mendillo, V. (2007). *Diplomado Seguridad en Redes*. Caracas, Venezuela. Universidad Metropolitana.

Mujica, M. (2012). *Curso de Seguridad de la Información*. Barquisimeto, Venezuela: Universidad Centroccidental “Lisandro Alvarado”.

Mujica, M., Álvarez Y. (sf). *El análisis de riesgo en la seguridad de la información*. Barquisimeto, Venezuela: UNEXPO, UPEL-IPB.

Piattini, M. (2001). *Auditoría informática, un enfoque práctico.* Mexico: Alfa Omega.

Universidad EAFIT (sf). *Consultoría Contable* [Documento en línea]. Disponible: http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/Nota%20de%20Clase%2021%20NAGA%C2%B4s.pdf. [Consulta: 2014 agosto 14].

ANEXOS

ANEXO A
TAXONOMÍA DE BLOOM

TABLA DE VERBOS DIDACTICOS DE LA TAXONOMIA DE BLOOM Que se utilizan en la elaboración de objetivos, de acuerdo a las categorías de dominio cognitivo. El verbo no es la base de la taxonomía, Sino el nivel lógico, psicológico y pedagógico que abarca el objetivo esperado en el alumno.

CONOCIMIENTO	COMPRENSION	APLICACIÓN	ANALISIS	SINTESIS	EVALUACION
Abocar	Argumentar	Aplicar	Analizar	Agrupar	Acordar
Apuntar	Asociar	Aprovechar	Abstraer	Arreglar	Apreciar
Citar	Codificar	Calcular	Aislar	Aprestar	Aprobar
Definir	Comprobar	Cambiar	Calcular	Categorizar	Apoyar
Describir	Concluir	Construir	Categorizar	Clasificar	Calificar
Designar	Contrastar	Comprobar	Contrastar	Compilar	Categorizar
Determinar	Convertir	Delinear	Criticar	Componer	Comparar
Distinguir	Concretar	Demostrar	Comparar	Combinar	Concluir
Enumerar	Criticar	Describir	Debatir	Concebir	Contrastar
Enunciar	Deducir	Despejar	Describir	Construir	Criticar
Escribir	Definir	Determinar	Descomponer	Conceptuar	Defender
Explicar	Describir	Discriminar	Designar	Crear	Demostrar
Exponer	Demostrar	Diseñar	Detallar	Dirigir	Descubrir
Identificar	Discriminar	Distinguir	Determinar	Diseñar	Decidir
Indicar	Descodificar	Dramatizar	Descubrir	Distribuir	Elegir
Escribir	Discutir	Ejemplificar	Desglosar	Ensamblar	Escoger
Jerarquizar	Distinguir	Eliminar	Detectar	Elegir	Estimar
Enlistar	Ejemplificar	Emplear	Diferenciar	Erigir	Evaluar
Localizar	Estimar	Encontrar	Discriminar	Escoger	Explicar
Marcar	Explicar	Esbozar	Distinguir	Estimar	Fundamentar
Mencionar	Expresar	Estimar	Dividir	Esquematizar	Integrar
Mostrar	Extrapolar	Estructurar	Enunciar	Estructurar	Justificar
Nombrar	Generalizar	Explicar	Especificar	Evaluar	Juzgar
Reconocer	Identificar	Ilustrar	Examinar	Explicar	Medir
Registrar	Ilustrar	Interpolar	Experimentar	Exponer	Modificar
Relatar	Inferir	Inventariar	Explicar	Formular	Opinar
Recordar	Interpretar	Manejar	Fraccionar	Fundamentar	Precisar
Referir	Jerarquizar	Manipular	Identificar	Generar	Probar
Repetir	Juzgar	Medir	Ilustrar	Justificar	Revisar
Reproducir	Localizar	Modificar	Inferir	Juzgar	Reafirmar
Seleccionar	Narrar	Mostrar	Investigar	Inventariar	Refutar
Señalar	Ordenar	Obtener	Omitir	Medir	Relacionar
Subrayar	Organizar	Operar	Relacionar	Modificar	Seleccionar
	Opinar	Organizar	Seleccionar	Narrar	Sustentar
	Parafrasear	Practicar	Señalar	Organizar	Tasar
	Predecir	Preparar	Separar	Planear	Valorar
	Pronosticar	Probar	Seccionar	Probar	Valuar
	Reafirmar	Producir	Reflexionar	Producir	Verificar
	Relacionar	Relacionar		Programar	
	Resumir	Representar		Proponer	
	Revisar	Resolver		Proyectar	
	Sintetizar	Redactar		Reacomodar	
	Sostener	Tabular		Reconstruir	
	Transcribir	Trazar		Reunir	
	Traducir	Seguir		Reorganizar	
	Transformar	Transferir		Reparar	
		Usar		Refutar	
		Utilizar		Relacionar	
				Seleccionar	
				Sustentar	
				Valorar	
				Valuar	
				Verificar	

ANEXO B
INFORME FINAL

Grupo Metropolitano

Auditoría: Conectividad de Red

Identificación del Informe

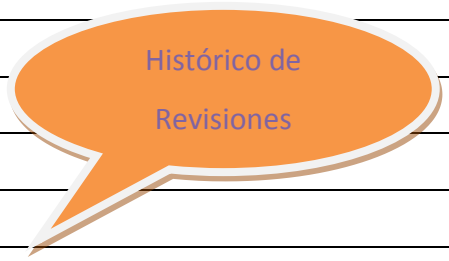
Documento:	DAI-AIR-1046
Revisión:	0
Fecha:	21/06/2013

Caracas, 2013

HISTÓRICO DE REVISIONES

Las revisiones que se han hecho de este procedimiento, las fechas y las causas son las siguientes:

NÚM. REV.	FECHA	HISTÓRICO DE REVISIONES
0	21/06/13	Primer Ejemplar



ÍNDICE GENERAL

Índice

Introducción

INTRODUCCIÓN

En la sociedad de hoy en día, es imposible negar la importancia que tiene la tecnología en el desempeño de las actividades diarias de las organizaciones, pues no sólo permite automatizarlas, haciendo más rápidas las labores, sino que además reduce, en parte, el riesgo de producir información errónea a partir de un error humano. Sin embargo, al igual que cualquier otro procedimiento, las tecnologías utilizadas como las redes y los equipos que implican, también deben pasar por un proceso periódico de mantenimiento, para garantizar que funcionen correctamente los servicios que presta (internet, intranet, telefonía, periféricos, entre otros) y permitan la consistencia y fiabilidad de los datos que a través de ella se envían y reciben.

Actualmente por la necesidad creciente de facilitar las operaciones empresariales, cualquier organización desde las más grandes a las más pequeñas, utilizan las redes informáticas. Sin embargo cabe preguntarse ¿Son las redes simples instrumentos para compartir recursos?, ¿Están las organizaciones conscientes de la necesidad de mantener sus redes en buen estado?, ¿Conocen los riegos que implica una red vulnerable que no cumple con los requerimientos mínimos de seguridad?

El proceso de auditoría informática en el área de redes, permite dilucidar estas inquietudes, que surgen como consecuencia de fallos, inestabilidad en una red empresarial o del proceso de análisis de su comportamiento, identificando así los procedimientos que a efectos de su instalación, mantenimiento y ampliación se estén realizando en forma inadecuada, dejando en blanco y negro una serie de recomendaciones para corregirlos y de esta forma hacer que el funcionamiento de esta delicada área, esté en óptimos niveles y a la par de los estándares internacionales definidos para tal fin.

Con el objetivo antes planteado, la auditoría informática de redes, consiste en la aplicación de instrumentos y procedimientos estandarizados, apropiados y adaptados a casa caso particular, para la colección de hallazgos y presentación de propuestas que permitan reforzar o corregirlos dependiendo de su naturaleza.

A continuación, se presenta el caso de auditoría informática de redes, practicado a la empresa "Grupo Metropolitano", un importante consorcio dedicado a diversas actividades económicas, asentado en el Distrito Capital, Venezuela. Dentro de éste se reflejan diversos aspectos que se exponen de la siguiente manera y llevando un orden secuencial del mismo con las normativas necesarias para su presentación, obteniendo así el Informe Final, que explica los resultados obtenidos luego de la realización de la auditoria informática de redes.

INFORME FINAL

Entidad Auditada:

Grupo Metropolitano.

Identificación de la Entidad Auditada

Área Auditada:

Departamento de Sistemas.

Identificación del Cliente

Tiempo estimado:

120 Horas.

Alcance:

Auditoría Informática de Redes (Conectividad).

Alcance de la Auditoría

Objetivos

Objetivo General:

Realizar una auditoría informática de red, en la empresa Grupo Metropolitano, para la gestión de interconexión (enlaces de datos) entre su Sede Central y Sucursales remotas.

Objetivos Específicos:

- Diagnosticar la situación actual de la gestión de la interconexión de datos entre su Sede Central y Sucursales remotas en la empresa Grupo Metropolitano.
- Analizar los servicios de red entre su Sede Central y Sucursales remotas en la empresa Grupo Metropolitano.
- Analizar la información recolectada durante el proceso de Auditoría Informática de Redes.
- Presentar informe del proceso de Auditoría Informática de Redes.

Hallazgos:

- La organización no cuenta con la capacitación y adiestramiento para que el personal que labora en esta área pueda realizar el mantenimiento de las redes.
- Contratación de terceros para la instalación y actualización de equipos, lo cual pone en riesgo a la información y la seguridad de la empresa, además de la dependencia que esto genera.
- Posible Acceso indebido al área de redes.
- Falta de procedimientos para la organización e identificación de equipos y dispositivos que conforman la red.
- Inexistencia de planos de las redes de la empresa, donde se indique los equipos, cableado y puntos de red instalados en todas las áreas.
- Inexistencia de un sistema automático que alerte sobre incidencias o ataques a la plataforma de red.
- Los parámetros de seguridad de los servidores son deficientes, lo cual vuelve frágil la protección lógica de las redes.

Conclusiones:

De manera general hemos determinado que los controles existentes sobre los recursos de la red del área local de la organización deben ser mejorados puesto que presentan grandes problemas para asegurar los nodos de la red antes de que estos accedan a la misma. Por otra parte se evidencia que el flujo u optimización de tráfico de red entre las sucursales del grupo metropolitano es deficiente por lo cual se debe trabajar para garantizar que las acciones de los usuarios son las correctas, desde el punto de vista de las responsabilidades y así evitar también el desvió de información.

Por todos los elementos antes expuestos que se han cumplido con los objetivos planteados y se ha logrado diagnosticar el estado actual de la gestión de interconexión de datos entre la sede central y sucursales remotas del grupo metropolitano.

- Se evidencia que el tráfico de red entre las sucursales del grupo metropolitano es deficiente por lo cual se debe trabajar para garantizar que las acciones de los usuarios son las correctas, desde el punto de vista de las responsabilidades y así evitar también el desvío de información.
- Se determinó que la seguridad en los cuartos de cableado deben ser mejorado.

Recomendaciones:

- Se recomienda a la Gerencia de Sistemas, colocar los centros de cableado en lugares adecuados, fuera del alcance de personas no autorizadas.
- Se recomienda a la Gerencia de Sistemas, identificar los dispositivos principales de la red.
- Se recomienda a la Gerencia de Sistemas, establecer y difundir las políticas y procedimientos, necesarios para proteger los recursos informáticos de la red de área local de la organización.
- Se recomienda a la Gerencia de Sistemas, evaluar periódicamente los permisos de acceso a la red y uso de recursos de telecomunicaciones.
- Se recomienda a la Gerencia de Sistemas, mejorar los controles existentes sobre los recursos de la red de área local de la organización.
- Se recomienda a la Gerencia de Sistemas, entrenar periódicamente al personal de IT de la organización en nuevas prácticas de gestión de redes.
- Se recomienda a la Gerencia de Sistemas, monitorear la red periódicamente, revisar los errores o situaciones anómalas que se producen, para evitar un daño interno.

Dictamen de Auditoría:

Nuestra opinión es que, los controles sobre los recursos de la red de área local de la organización deben ser mejorados puesto que presenta importantes dificultades. Esto se debe a la ausencia de lineamientos claros para su gestión.

Fecha del Informe

	Planificación	Ejecución	Informe
Fechas	03/06/13 al 07/06/13	10/06/13 al 14/06/13	17/06/13 al 21/06/13

Identificación y firma de los auditores

Apellidos y Nombres	Cargo	Firma
Ing. Marco López	**Auditor Sénior**	
Ing. José Figueredo	**Auditor Sénior**	
Ing. Manuel Castillo	**Auditor Sénior**	

ANEXO C

PRÁCTICA SOBRE AUDITORIA DE SEGURIDAD PARA REDES Y SERVICIOS

PRÁCTICA SOBRE
AUDITORÍA DE SEGURIDAD PARA REDES Y SERVICIOS

Objetivo

Familiarizarse con algunas de las técnicas y herramientas utilizadas para encontrar y evaluar las vulnerabilidades y brechas de seguridad existentes en una red y en los servicios que corren en las computadoras, con la finalidad de implantar las medidas defensivas apropiadas.

Introducción

¿Qué es la auditoría de seguridad?
Es el examen o revisión de carácter objetivo, crítico y sistemático de la seguridad física, técnica y administrativa con el objetivo primordial de evaluar el grado de protección que existe contra posibles amenazas y riesgos. Se trata principalmente de verificar si se están aplicando las medidas de control más apropiadas para asegurar la integridad, confidencialidad y disponibilidad de la información.

Con una auditoría global se obtiene una radiografía completa de los activos de información, en cuanto a protección y medidas de seguridad. También puede efectuarse la auditoría de un aspecto determinado (ej. servidor Web).

La auditoría de la seguridad física se ocupa de la revisión del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. En este caso se analizan situaciones como incendio, inundación, sabotaje, robo, catástrofe natural, etc. En este tipo de auditoría se revisan, por ejemplo: control de acceso, identificación, instalaciones, datacenters, servidores, medios y procesos de almacenamiento, etc.

La auditoría de seguridad lógica (o técnica), tiene que ver con los controles para el uso de software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. Cubre los siguientes aspectos: arquitecturas, servidores (Windows, Unix y Linux), reglas de filtrado del firewall, configuración de electrónica y tráfico LAN/WAN.

Un aspecto importante de la auditoría de la red, es la detección de brechas y puntos débiles que puedan ser aprovechados por intrusos (externos o internos). De ser así, existe un alto riesgo de que datos importantes o confidenciales puedan ser sustraídos o de que queden fuera de servicio operaciones vitales, perdiéndose así tiempo, prestigio y dinero.

Una buena infraestructura de seguridad, con un plan maestro que incluya políticas, normas y procedimientos, así como la implantación de cortafuegos (*firewalls*), sistemas de detección de intrusos (IDS) y sistemas de control de acceso, no garantiza una protección completa.

El problema que se plantea entonces es: ¿Cómo averiguar que no existan vulnerabilidades y fallas de seguridad? ¿Cómo saber si hay suficiente protección contra las nuevas técnicas de ataque utilizadas por los hackers o por los propios empleados? ¿Cómo estar seguros que cambios de configuración o la instalación de nuevos programas no han abierto una nueva brecha?

La primera fase de la verificación de la seguridad es identificar las vulnerabilidades y brechas existentes. En el nivel más simple, una brecha de seguridad aparece simplemente abriendo un puerto tal como 25 (servidor SMTP de correo) o 80 (servidor Web). Esto, por supuesto, no significa necesariamente que represente un riesgo, ya que hoy muchos otros factores estan involucrados. Además, los riesgos pueden ser reducidos por medio de firewalls y sistemas de detección de intrusos (IDS). Pero las brechas de seguridad aparecen por muchas otras vías. Como un ejemplo, al permitir que los empleados reciban e-mails o que naveguen por Internet, se abren brechas por donde pueden entrar virus y hackers mediante puertas traseras.

Mediante la auditoría de seguridad de la red se buscan vulnerabilidades en enrutadores, firewalls, switches, hubs, servidores Web, servidores de correo, servidores FTP, estaciones de trabajo, impresoras, etc., servicios con puertas traseras conocidas, *exploits* de los protocolos TCP/IP, entrada remota al registro en Windows, servicios remotos (rlogin, rsh, NFS) y mucho más.

Este proceso puede que signifique tener que chequear montones de posibles brechas para centenares de aplicaciones y docenas de sistemas operativos. Por ejemplo, se requiere revisar los distintos sistemas de información (SQL, Oracle, Sybase) buscando configuraciones erróneas que pueden conducir a fuga o hurto de datos. Por tal razón se requiere tener al día una base de datos de vulnerabilidades y *exploits*, la cual crece a una tasa de decenas de nuevas alertas por semana.

Una etapa crucial de la auditoría de seguridad son las *pruebas de penetración*, las cuales esencialmente consisten en tratar de violar la seguridad y penetrar en una red o sistema, aprovechándose de los puntos débiles encontrados, tal como lo haría un hacker o un empleado interno malintencionado.

Las pruebas de penetración pueden durar horas, días o semanas y usualmente se realizan desde el exterior de la red, pero se pueden realizar también desde el interior de la red para evaluar las defensas en la eventualidad de que sucumban las protecciones externas o contra ataques internos desde máquinas locales.

Mediante las llamadas “pruebas a ciegas” se utiliza solamente información de carácter público disponible sobre el blanco, simulando así las actividades de los hackers desde Internet.

En cambio, mediante las “pruebas con pleno conocimiento”, se utiliza toda la información disponible, por ejemplo, sobre la topología de la red y la configuración de los sistemas. Así se garantiza que todo equipo que se encuentre conectado a la red sea inspeccionado y evaluado. Es de hacer notar que

aproximadamente el 80% de las violaciones de seguridad se basan en información interna.

Los especialistas en estas pruebas (también conocidos como *hackers éticos*) hacen uso de tres tipos de herramientas:

1. Las que se consiguen libremente en Internet (como Nmap y Nessus) y que son comúnmente usadas por los hackers.
2. Las de tipo comercial (como ISS, Retina, SSS), las cuales permiten hacer pruebas sistemáticas y automatizadas.
3. Las desarrolladas por los propios especialistas en seguridad.

La experiencia ha demostrado que las herramientas para pruebas automatizadas logran detectar algo más del 50% de las fallas, pero el resto se detecta mediante pruebas manuales. Por otro lado éstas fallas son a menudo más graves que las otras.

En el caso de que durante las pruebas se detecten problemas serios o actividades ilícitas (por ejemplo, presencia de hackers o intrusos), se debe notificar de inmediato al personal de seguridad de la empresa, para así, tomar medidas correctivas y preventivas.

Resultados

Los resultados de la auditoría de seguridad se deben reportan en un informe confidencial, claro y bien estructurado, donde se detallan todas las vulnerabilidades encontradas, con sus correspondientes comentarios en cuanto a las posibles implicaciones asociadas y las correspondientes acciones correctivas recomendables.

El informe debe contener un análisis descriptivo junto con aspectos técnicos que ayuden a comprender los problemas existentes y cómo subsanarlos.

Metodología

Existen diferentes metodologías para llevar a cabo una auditoría de seguridad y OSSTMM (*Open Source Security Testing Methodology Manual*) es, entre los productos no comerciales, quizás uno de los más completos existente en la actualidad.

Esta metodología, desarrollada por el Instituto ISECOM liderizado por Peter Herzog, se encuentra en constante evolución y es fruto de la colaboración de más de 150 personas en todo el mundo. Gracias a este gran número de colaboradores, el documento incorpora los más recientes cambios y nuevos desarrollos relacionados con la seguridad informática.

Antes de OSSTMM no existía ningún documento público que recogiera, de forma abierta y estandarizada, las diferentes necesidades del profesional de la seguridad durante la realización de la auditoría de seguridad. Si bien existen otras metodologías (por ejemplo ISO 27001 y COBIT), ninguna es tan específica y con la intención de estar disponible y mantenida por la propia comunidad de profesionales en seguridad.

OSSTMM ofrece un marco de referencia así como unos resultados claramente cuantificables. Gracias a esto, es posible garantizar los resultados, la exactitud y la validez de las pruebas realizadas.

OSSTMM es sumamente útil para los profesionales de seguridad informática así como para los administradores de redes, y define una serie de acciones a realizar en las pruebas de penetración, "hacking ético" y verificación de la seguridad de los activos de información. El objetivo, pues, es ofrecer un marco estandarizado para la evaluación de la seguridad.

Para el desarrollo del manual se tomaron en cuenta diversas normativas legales (entre las que se incluye la ley española de protección de datos), de forma que OSSTMM también puede ser utilizada en la evaluación del cumplimiento de las mismas. El proceso de realización de pruebas descrito en la metodología, incluye los siguientes ámbitos:

1. Análisis de la red
2. Análisis de puertos
3. Identificación de sistemas
4. Pruebas de debilidades en sistemas inalámbricos
5. Verificación de servicios (Web, correo, servidor de nombres, documentos visibles, virus y troyanos)
6. Determinación de vulnerabilidades
7. Identificación de exploits
8. Verificación manual de vulnerabilidades
9. Verificación de aplicaciones
10. Verificación de cortafuegos y ACL
11. Revisión de la política de seguridad
12. Revisión de sistemas de detección de intrusos
13. Revisión de sistemas de telefonía
14. Obtención de información (servicios de noticias, notas de prensa, informaciones facilitadas por la propia empresa), ofertas de trabajo, newsgroups, xracks, números de serie y "underground", FTP, Web, P2P
15. Ingeniería social
16. Verificación de sistemas "confiables"
17. Análisis de fortaleza de contraseñas
18. Negación de servicio
19. Revisión de la política de privacidad.
20. Análisis de cookies y bugs en la Web
21. Revisión de archivos de anotaciones cronológicas (logs)

Por otro lado y sin ninguna relación con OSSTMM, el *Computer Security Resource Center,* organismo que depende del NIST (*National Institute of Standards and Technology*) del Departamento de Comercio de los Estados Unidos ha publicado su metodología para la verificación de la seguridad de los sistemas y de las políticas de seguridad. Este documento está dividido en cuatro secciones: una introducción a la metodología, la descripción de los métodos de verificación y el conjunto de seguridad, la definición de los métodos y objetivos de las pruebas de seguridad y, en la última sección, qué elementos deben tener prioridad cuando se realizan las verificaciones con recursos limitados.

En las experiencias prácticas que siguen a continuación se van a tratar algunos de los aspectos antes mencionados y principalmente lo referente a la determinación de vulnerabilidades.

El procedimiento que vamos a utilizar se basa en varias fases o etapas:

1. Fase de recopilación de información general (*reconnaissance and footprinting*) sobre el blanco (*target*).
2. Fase de recopilación específica sobre las redes y sistemas informáticos.

3. Fase de exploración y barrido (*scanning*) de las redes y sistemas informáticos, para encontrar eventuales vulnerabilidades.
4. Fase de análisis de las vulnerabilidades y brechas de seguridad encontradas.
5. Fase de ataques (pruebas de penetración y negación de servicio) para explotar las vulnerabilidades encontradas (*exploit*). Esta fase no siempre se lleva a cabo, ya que puede afectar el funcionamiento de los equipos y sistemas.
6. Fase de elaboración de informe, explicando los riesgos y las posibles consecuencias, con recomendaciones para remediar las vulnerabilidades.

Para cada una de las fases se debe guardar el registro de auditoría (*log*) con los resultados, a fin de incluirlos en el informe final.

Fase 1: Recopilación de información general

Aquí se trata de recabar tanta información como sea posible sobre el blanco. Mediante la evaluación a ciegas se utiliza sólo el nombre de la organización, sin ninguna ayuda desde adentro, para así simular la situación de un ataque de intrusos desde Internet.

En primer lugar se averigua lo que más se pueda sobre el perfil de la organización, por ejemplo: ámbito de actividades, sedes y sucursales, proveedor de Internet (ISP), personas claves, servicios que se ofrecen, etc. Para esto pueden usarse las siguientes modalidades:

a) *Búsqueda en el Web*: Se utiliza un motor de búsqueda como Google o Altavista y luego se visita el sitio Web de la organización.
b) *Consulta Whois*: Se contacta una base de datos Whois para identificar la ubicación física, los nombres y teléfonos del contacto administrativo y técnico, los servidores de nombre de dominio (DNS), etc. Existen utilidades para todas las plataformas para llevar a cabo una solicitud Whois sobre un dominio, aunque sólo está disponible de forma nativa bajo Unix y Linux. Afortunadamente, existen herramientas (por ejemplo, *IP_Tools* que permiten usar Whois bajo Windows. Además hay varios sitios Web que ofrecen el servicio Whois, por ejemplo *http://www.allwhois.com* que es uno de los más completos. Alternativamente se pueden utilizar los siguientes más específicos:

   Estados Unidos (dominios .aero, .arpa, .biz, .com, .coop, .edu, .info, .int, .museum, .net, .org):
   http://www.internic.com
   http://www.arin.net
   http://www.networksolutions.com

   Europa: *http://www.ripe.net*

   Latinoamérica: *http://lacnic.net*

   Venezuela (dominios .ve): *http://www.nic.ve*

c) *Consulta a hosts*: Se trata de identificar el tipo de equipo o sistema existente y las personas a cargo del mismo mediante herramientas como: rusers, finger, showmount, rpcinfo, nslookup, host, traceroute, telnet, etc.
d) *Consulta de servicios*: Se utiliza el DNS para identificar los servicios que se suministran, las direcciones IP y cualquier otra información relevante. En particular se intenta identificar sendmail (SMTP), ftp, www, proxy, etc.

Se puede conseguir mucha Información adicional en sitios como estos:

www.google.com
www.securityfocus.com
www.snpx.com
www.hispasec.org
www.dodomex.com
www.cert.org
www.sans.org
www.sectools.org
www.cpiu.us
www.milw0rm.com
www.metasploit.com

1. Como ejemplo de recopilación de información sobre una posible blanco u objetivo, buscaremos en Google las empresas que venden al detal y por remate. Allí conseguimos, entre otros sitios Web, a *www.deremate.com*.

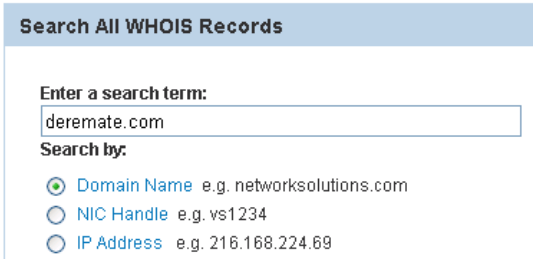
Visitamos el sitio, donde aparecen enlaces a sucursales de varios países latinoamericanos. Para Venezuela, es *venezuela.deremate.com.*

Nota: Trate de repetir las experiencias que siguen con este sitio u otro que usted escoja, por ejemplo, *http://tucarro.com*.

A continuación consultamos Whois en *http://www.internic.com* buscando información sobre el dominio *deremate.com* y obtenemos los siguientes resultados:

```
Domain Name: DEREMATE.COM
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: MAIL.DEREMATE.COM
Name Server: MAIL01.DEREMATE.COM
Name Server: LUTHOR.US.IMPSAT.NET
Status: REGISTRAR-LOCK
Updated Date: 24-oct-2004
Creation Date: 11-jun-1999
Expiration Date: 11-jun-2006
```

Como el Registrar es Network Solutions, consultamos Whois en este enlace: *http://www.networksolutions.com* obteniendo entonces mucho más información:




```
Registrant: Make this info private
 DEREMATE.COM, Inc.
 201 South Biscayne Blvd.
 28 fl.
 Miami, FL 33131
 US

 Domain Name: DEREMATE.COM

 Administrative Contact :
 Garcia, Pablo
 administrative@deremate.com
 Maipu 942 15
 Buenos Aires, Cap Fed 1006
 AR
 Phone: 54 11 4893 1222
 Fax: 54 11 4893 1444

 Technical Contact :
 Garcia, Pablo
 technical@deremate.com
 Maipu 942 15
 Buenos Aires, Buenos Aires 1006
 AR
 Phone: 54 11 4893 1222
 Fax: 123 123 1234

 Record expires on 11-Jun-2006
 Record created on 11-Jun-1999
 Database last updated on 07-Jul-2004

 Domain servers in listed order: Manage DNS

 MAIL.DEREMATE.COM 200.41.112.112
 MAIL01.DEREMATE.COM 200.41.112.110
 LUTHOR.US.IMPSAT.NET 200.31.7.4
 DNS04.EXODUS.NET 209.1.222.247
```

Llegados a este punto, es necesario convertirse en un detective cibernético. Se debe analizar la información buscando pistas que proporcionen más información, por ejemplo, la ubicación geográfica de la sede principal y de las sucursales. El contacto administrativo es una pieza importante de la información, ya que permite averiguar el nombre de la persona responsable de la conexión a lnternet o del firewall. También a menudo se listan números de teléfono y de fax. Esta información es de gran ayuda cuando se esté llevando a cabo una revisión de penetración por vía telefónica, por ejemplo mediante los llamados "discadores de guerra" (*war dialers*). Además, con frecuencia, un intruso puede hacerse pasar por un contacto administrativo utilizando "ingeniería social" con usuarios que estén libres de toda sospecha dentro de la organización. El atacante enviará correos electrónicos falsos a usuarios ingenuos haciéndose pasar por el administrador. Es asombrosa la cantidad de usuarios que cambian su contraseña por la que el intruso le proporciona, siempre y cuanto parezca que se lo pide una persona de confianza de departamento de soporte al usuario.

Las fechas de creación y de actualización del registro revelan si la información es todavía válida. Si el documento fue creado hace cinco años y no ha sido actualizado desde entonces, es fácil apostar a que alguna parte de la información (por ejemplo, el contacto administrativo) puede estar obsoleta.

La última parte del listado proporciona información sobre los servidores DNS autorizados. El primero de la lista es el servidor principal, los siguientes serán el secundario, el terciario, y así sucesivamente. Se necesitará esta información para las consultas de DNS que se tratarán en detalle más adelante.

Gran parte de la información contenida en varias de las bases de datos anteriormente mencionadas es totalmente pública. Cuando una empresa registra un dominio en Internet necesita contactos administrativos, bloques de red registrados e información del servidor de nombres autorizado. Sin embargo, se deberían utilizar ciertas medidas de seguridad para dificultar el trabajo de los atacantes.

Muchas veces, un contacto administrativo abandona la empresa y sigue siendo capaz de cambiar la información que aparece en InterNIC sobre la misma. Así pues, lo primero que uno debería hacer, es asegurarse de que la información existente en la base de datos es confiable. Debe actualizarse la información relacionada con el contacto administrativo, técnico y de facturación cuando sea necesario. Más aún, deberían tenerse en cuenta los números de teléfono y direcciones listados, ya que pueden utilizarse como punto de partida para ataques telefónicos o con fines de ingeniería social. Debería utilizarse un número de teléfono gratuito o un número de teléfono que no se encuentre en la centralita telefónica (PBX) de la empresa. También se podría usar un contacto administrativo ficticio, esperando de esta forma descubrir a alguien que esté intentando llevar a cabo una labor de ingeniería social, de manera que si algún empleado recibe un correo electrónico o una llamada por parte del supuesto administrador, el departamento de seguridad de la información podría ponerse en alerta.

2. Otra forma de usar el servicio Whois es mediante herramientas como *IP-Tools* para así interrogar servidores Whois, tales como los siguientes:

whois.networksolutions.com
whois.internic.net
whois.lacnic.net
whois.arin.net
whois.nic.mil
whois.nic.gov
whois.ripe.net

3. Corra IP-Tools y seleccione la utilidad *WhoIs*. En la casilla *Server* coloque *whois.networksolutions.com* y en la casilla *Query* coloque *deremate.com*. Debería obtener la misma información que vimos antes. Nota: Para dominios .ve de

Venezuela deberá hacer la consulta al server *whois.nic.ve* administrado por el CNTI (Centro Nacional de Tecnologías de Información).

4. La base de datos ARIN permite averiguar a quién ha sido asignada una dirección IP. En la casilla *Server* coloque *whois.arin.net* y en la casilla *Query* coloque la dirección IP de MAIL.DEREMATE.COM, que es 200.41.112.112. Obtendrá algo como lo siguiente:

```
OrgName: Latin American and Caribbean IP
address Regional Registry
OrgID: LACNIC
Address: Potosi 1517
City: Montevideo
StateProv:
PostalCode: 11500
Country: UY
ReferralServer: whois://whois.lacnic.net
NetRange: 200.0.0.0 - 200.255.255.255
CIDR: 200.0.0.0/8
NetName: LACNIC-200
NetHandle: NET-200-0-0-0-1
Parent:
NetType: Allocated to LACNIC
NameServer: NS.LACNIC.NET
NameServer: TINNIE.ARIN.NET
NameServer: NS-SEC.RIPE.NET
NameServer: SEC3.APNIC.NET
NameServer: NS2.DNS.BR
Comment: This IP address range is under LACNIC
responsibility for further
Comment: allocations to users in LACNIC
region.
Comment: Please see http://www.lacnic.net/ for
further details, or check the
Comment: WHOIS server located at
whois.lacnic.net
RegDate: 2002-07-27
Updated: 2005-03-29
```

5. Una forma indirecta de usar Whois es mediante herramientas como Neotrace. Corra este programa y en la casilla *Target* ponga *www.deremate.com*. Al completarse el descubrimiento de la ruta, vaya al último nodo mediante el botón *Next*. Vea la información bajo *Summary, Registrant, Network y Timing*. Compare con la información obtenida directamente mediante Whois.

6. A continuación utilice algunas de las técnicas anteriores para recopilar información sobre entes y organizaciones como los siguientes (u otros que se le ocurran). Nota: Para dominios .ve de Venezuela deberá hacer la consulta al servidor *whois.nic.ve* administrado por el CNTI (Centro Nacional de Tecnologías de Información). Ver también *http://www.nic.ve*.

yahoo.com
microsoft.com
cantv.net
pdvsa.com
banesco.com
bancodevenezuela.com
bancomercantil.com
provinet.net
mercadolibre.com.ve
www.auyantepui.com.ve
biv.com.ve
movilnet.com.ve
movistar.com.ve
ucv.edu.ve
unimet.edu.ve
ucab.edu.ve
conatel.gov.ve
platino.gov.ve
venezuela.gov.ve
www.seniat.gov.ve
www.mf.gov.ve
gobiernoenlinea.ve
www.mij.gov.ve
mre.gov.ve
asambleanacional.gov.ve

Fase 2: Recopilación de información específica

En esta fase se trata de obtener información específica detallada sobre la topología de la red, así como la configuración y características de cada equipo, de tipo de servidores, sistemas operativos (versión, service pack, parches), direcciones IP, mapa de la red, etc. Para las pruebas con pleno conocimiento se puede solicitar y recabar información como la siguiente:

a) Lista completa de direcciones de IP asignadas, sean utilizadas o no.
b) Inventario de todos los equipos conectados en red, especificando los siguientes datos: nombre del host, función que cumple, dirección IP, descripción del hardware, sistema operativo y service pack (o parche).
c) Planos y diagramas de la red, apoyados eventualmente de información obtenida del sistema de gestión, si existe.

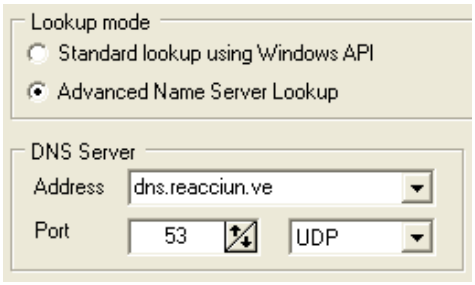
El siguiente es un listado parcial de la información que se obtendría (total o parcialmente) al final de la etapa de identificación:

- Cobertura de la red y gama de direcciones IP.
- Puntos de acceso a la red
- Redes privadas e intranets
- Nombres de las máquinas y de los servidores (http, mail, ftp, etc.)
- Equipos de red y marca:
  - Routers, switches y hubs (por ejemplo: Cisco, 3Com, Nortel, Cabletron, Lucent)
  - Sistemas operativos (por ejemplo: Windows NT4.0, Windows 2000, Windows XP, Windows 9x, Linux, BSD, MacOS X, Solaris, HP-UX, Irix, AIX, SCO, Novell)
  - Firewalls (por ejemplo: CheckPoint Firewall-1, Novell Border Manager, TIS, CyberGuard, IPchains)
  - Servidores Web (por ejemplo: Apache, Microsoft IIS, Lotus Domino, Netscape Enterprise, IpSwitch, WebSite Pro)

- Servidores FTP (por ejemplo: IIS FTP Server, WuFTPd, WarFTPd)
- Servidores LDAP (por ejemplo: Netscape, IIS, Domin,Open LDAP)
- Servidores para balanceo de carga (por ejemplo: IBM Network Dispatcher, Intel, Resonate Central Dispatch, F5, ArrowPoint, Alteon)

1. Desde el menú de IP-Tools seleccione *Tools* | *Lookup.* En *Host* ponga *reacciun.ve*.

2. Seleccione *Options,* en *Lookup mode* seleccione *Advanced* y en DNS server ponga *dns.reacciun.ve*



3. Pulse *Start* y analice la respuesta y en particular el significado de: authoritative o non-authoritative answer, A, MX, NS, SOA, IN (según se explica más adelante).

4. Repita la experiencia anterior con servidores de nombres (por ejemplo *dns.cantv.net*, *ns1.worldnet.att.net, ns1.midspring.com, ns1.kloth.net*) y otros dominios, por ejemplo:

hotmail.com
yahoo.com
ucv.ve
unimet.edu.ve
cantv.net

5. Explicación: Los servidores DNS no contienen información de todas las computadoras existentes en Internet. En lugar de ello, tienen autoridad únicamente sobre determinadas subredes y contienen sólo la información de los nombres de host de estas subredes. También disponen de la capacidad de consultar información de otros servidores DNS y así dar respuesta a solicitudes referentes a máquinas sobre las que no tienen autoridad. Para minimizar el tráfico de red, la mayoría de los servidores DNS guardan en caché la información sobre otros servidores y responderán a las solicitudes directamente, como si ellas tuvieran autoridad sobre las subredes remotas. Sin embargo, deberán identificar su respuesta como no-vinculante. Para mantener la información almacenada en la caché del DNS actualizada, cada elemento de la base de datos DNS tiene un tiempo de vida (Time To Live, TTL) específico. Una vez que el TTL ha transcurrido, el elemento se borra de la caché. El TTL suele estar configurado a varias horas, ya que los nombres de host suelen ser relativamente estables.

La resolución de nombres puede ser un proceso muy costoso en términos de tiempo de proceso. Aunque la mayoría de los nombres se resuelven en una fracción de segundo, el tiempo de proceso depende por completo de lo rápido que puedan responder los servidores DNS primarios de dominio a una solicitud. Para reducir la carga del servidor de nombres, se puede configurar un servidor de caché en la red que ayude a aligerar de trabajo a los servidores primarios.

Aunque la mayoría de las resoluciones de nombres de host se efectuarán de forma transparente, de vez en cuando es útil el poder realizar búsquedas directas en un servidor de nombres. Si detectamos una cierta dirección IP en un archivo de registro, puede ser interesante obtener información sobre el nombre de la máquina, o sobre la subred en que se encuentra la máquina. Algunas de las solicitudes que podemos realizar al servidor son:

- A (*Address records*). Es el tipo más común de búsqueda. El registro de dirección es la dirección IP de un determinado nombre de host.
- CNAME (*Canonical name*). Proporciona un alias al nombre de host. Por ejemplo, si deseamos dar servicio FTP desde una máquina denominada www.poisontooth.com, podemos configurar un CNAME de ftp.poisontooth.com al nombre de host www y ambos se resolverán en la misma dirección.
- MX (*Mail Exchanger*). Los servidores de correo utilizan las entradas del intercambiador de correo para permitir que los mensajes dirigidos a un determinado nombre de host se puedan redirigir a un nombre diferente. Por ejemplo, si deseamos que el correo enviado a poisontooth.com se redirija a mail.poisontooth.com, podemos añadir un elemento MX para poisontooth.com que apunte a mail.poisontooth.com.
- NS (*Name Server*). Dado un nombre de dominio, una búsqueda NS devolverá los servidores de nombres que estén registrados para ese dominio.
- SOA (*Start of Authority*). El elemento SOA devuelto para un nombre de host nos indica cuál es el servidor de nombres que tiene autoridad sobre este nombre de host y el resto de máquinas del subdominio en que se encuentra. También proporciona información sobre el correo electrónico de la persona de contacto del subdominio e información variada relativa a los períodos de actualización de datos y cuándo ha sido la última vez que se han actualizado éstos (en segundos transcurridos). Ejemplo de valores:
  870729 (serial)
  1800 (refrescar cada 30 minutos)
  300 (reintentar cada 5 minutos)
  604800 (expira a la semana)

86400 (conservar mínimo un día)

Existen otros tipos de elementos de información en los servidores de nombres, como el elemento HINFO (Host Information), que rara vez se utilizan. La entrada HINFO se puede emplear para almacenar información sobre el hardware y configuración del sistema operativo de una determinada computadora. Este almacenamiento constituye un riesgo para la seguridad, debido a que se podrían preguntar al servidor de nombres y determinar los sistemas operativos más vulnerables, para lanzar ataques contra máquinas.

Si disponemos de un servidor de correo, es una buena idea tener elementos MX que apunten al servidor para todas las computadoras de nuestra red. De esta forma, se podría enviar correo a cualquier computadora de nuestra organización y siempre iría al servidor principal de correo, independientemente de la dirección utilizada.

Uno de las fallas de configuración más serias que un administrador del sistema puede cometer es permitir entrar en la *transferencia de zona* de DNS a usuarios de Internet no autorizados.

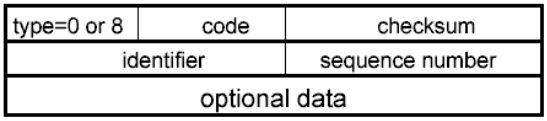
Una transferencia de zona permite que un servidor maestro secundario actualice su base de datos de zona a partir del servidor maestro primario. Esta operación se realiza por razones de redundancia de DNS, en caso de que el servidor principal de nombres deja de estar disponible en un instante determinado. En general, sólo los servidores maestros de DNS secundarios requieren realizar una transferencia de zona DNS. Sin embargo, muchos servidores de DNS están mal configurados y proporcionan una copia de la zona a cualquiera que se la pida. Esta situación no tiene por qué resultar necesariamente perjudicial si la información suministrada sólo hace referencia a los sistemas conectados a Internet y que tengan nombres de hosts válidos, aunque esto facilite a los atacantes la localización de objetivos potenciales. El problema real surge cuando una empresa no utiliza un mecanismo de DNS público/privado para separar su información de DNS externa (que es pública) de la interna, que es información DNS privada. En este caso, los nombres de hosts internos y las direcciones IP están a la vista de los atacantes. Suministrar información sobre las direcciones IP internas a un usuario de lnternet no autorizado es semejante a suministrarle un mapa completo de la red interna de una organización.

Existen muchas técnicas y herramientas que se pueden utilizar para llevar a cabo una transferencia de zona. Una forma sencilla es utilizar el cliente *nslookup*, que normalmente viene con los sistemas operativos Unix y Windows NT/2000.

Fase 3: Exploración y barrido (*scanning*)

Una vez que se hayan determinado las direcciones IP de las máquinas, se trata de averiguar si están activas y cuáles puertos están abiertos. Para tal fin se utilizan herramientas de dominio público y herramientas comerciales, algunas de las cuales también reportan el hallazgo de vulnerabilidades conocidas. Antes de usarlas, es importante actualizarlas para que se carguen con la lista de vulnerabilidades más recientes. Finalmente se hace un escaneo manual sobre cada dirección para así verificar y afinar los resultados del examen inicial. Aquí se pueden utilizar herramientas más refinadas como Nmap.

Para averiguar si las direcciones IP del blanco están activas, lo usual es llevar a cabo un barrido ping sobre esa gama de direcciones. Ping se utiliza tradicionalmente para enviar paquetes ICMP ECHO (Tipo 8), en un intento por obtener un ICMP ECHO REPLY (Tipo 0) que indique que el destino está activo.



Estructura de los mensajes ECHO

Aunque ping es aceptable para determinar el número de sistemas activos en una red pequeña, o de tamaño medio, no es eficiente para las redes corporativas de mayor tamaño. Para llevar a cabo exploraciones de grandes redes de Clase A, pueden ser necesarias varias horas, o incluso días.

Para realizar un barrido ping se puede utilizar una gran cantidad de herramientas, disponibles tanto para UNIX como para Windows.

ICMP es un excelente protocolo para diagnosticar problemas de red, pero también puede ser usado fácilmente con otros fines no tan lícitos. Si se permite un tráfico ICMP sin restricciones en el gateway (puerta de enlace) de frontera, los atacantes podrían llevar a cabo un ataque de negación de servicio (por ejemplo, Smurf).

En realidad existen 18 tipos de paquetes ICMP, de los cuales ECHO y ECHO_REPLY son únicamente dos de tales tipos. Aunque prácticamente cualquier cortafuego puede filtrar todos los paquetes ICMP, ciertas organizaciones pueden necesitar que el cortafuego deje pasar algún tráfico ICMP. Si existe realmente esa necesidad, se debe analizar cuidadosamente a qué tipo de tráfico ICMP va a permitir el paso. Una primera solución puede ser permitir únicamente el paso dentro de la red de paquetes ECHO_REPLY, HOST UNRECHABLE y TIME EXCEEDED.

Los barridos ping son apenas la punta del iceberg en lo que se refiere a la información ICMP de un sistema. Se puede reunir todo tipo de información valiosa sobre un sistema sin más que enviar un paquete ICMP. Por ejemplo, con la herramienta de UNIX, denominada *icmpquery*, se puede solicitar la hora del sistema para así ver en qué zona horaria está, enviando un mensaje ICMP de tipo 13 (TIMESTAMP). También se puede solicitar la máscara de red de un determinado dispositivo mediante un mensaje ICMP de tipo 17 (ADDRESS MASK REQUEST). La máscara de red de una tarjeta de red es importante debido a que se pueden determinar todas las subredes que se están utilizando. Conociendo las subredes, un hacker puede orientar sus ataques hacia una subred determinada y así evitar, por ejemplo, las direcciones de difusión (*broadcast*).

Uno de los mejores métodos de prevención es bloquear los tipos ICMP que suministran información a los routers de frontera. Al menos se debería restringir la entrada en la red de los paquetes TIMESTAMP (ICMP tipo 13) y ADDRESS

MASK (ICMP tipo 17). En los routers Cisco se puede evitar que respondan a estas solicitudes de paquetes ICMP estableciendo las siguientes ACL (*Access Control Lists*):

```
access-list 101 deny icmp any any 13
! petición de estampar la hora

access-list 101 deny icmp any any 17
! petición de máscara de direcciones
```

Luego del barrido ping, se procede a efectuar una exploración o escaneo de puertos TCP y UDP del blanco destino a fin de determinar qué servicios se están ejecutando o si el puerto está en un estado LISTENING (de escucha). Identificar los puertos que están a la escucha es fundamental para determinar el tipo de sistema operativo y aplicaciones en uso. Los servicios activos que estén a la escucha pueden permitir que un usuario no autorizado tenga acceso a sistemas que no estén bien configurados o que ejecuten una versión de software que tenga problemas de seguridad conocidos. Esta técnica consume bastante tiempo y no siempre es concluyente.

Son varios los objetivos perseguidos cuando se realiza una exploración de puertos del sistema destino. Entre estos objetivos se incluyen los siguientes:

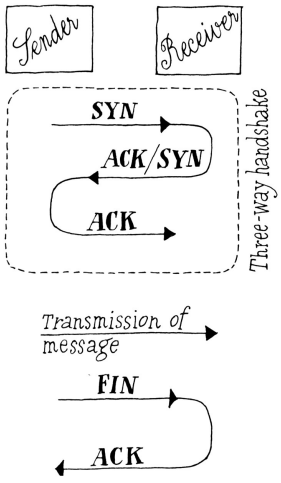
- Identificar los servicios TCP y UDP que se están ejecutando en el sistema objetivo.
- Identificar el tipo de sistema operativo del sistema objetivo.
- Identificar las versiones o aplicaciones específicas de un determinado servicio.

Nota: Escanear otras redes puede ser ilegal en algunos países y se podrían considerar los escaneos de puertos como ataques. Es posible que lleguen a molestar a alguna gente. Obtenga primero el permiso para hacerlo o hágalo bajo su propia responsabilidad. En todo caso cuando el tráfico ICMP se encuentra bloqueado, la exploración de puertos es quizás la mejor técnica para encontrar las máquinas activas.

Hoy día existen numerosas herramientas de exploración de puertos y uno de los pioneros en el desarrollo de las diversas técnicas es un personaje cuyo apodo es Fyodor y quien las ha incorporado en su famosa herramienta *Nmap*. Ella tiene la capacidad para realizar barridos ICMP y ofrece una opción más avanzada denominada *TCP ping scan* (exploración de ping TCP). Se puede efectuar un TCP ping scan mediante la opción -PT y un número de puerto, por ejemplo 80. Se emplea 80 porque es el puerto común usado por los routers de frontera para los sistemas de su misma zona desmilitarizada (DMZ) y, mejor aún, a través de sus cortafuegos principales. Esta opción enviará paquetes TCP SYN a la red destino y esperará la respuesta. Los host que estén activos contestarán con un paquete TCP SYN/ACK.

A continuación se describen las formas de exploración que realiza *Nmap* y otros productos comerciales sofisticados como SSS, ISS y *Cybercop*. Para más detalles lea los anexos al final de esta guía.

Exploración de conexión TCP. Este tipo de exploración conecta con el puerto objetivo y ejecuta un inicio de sesión completo de tres vías (SYN, SYN/ACK y ACK). Es fácilmente detectable por el sistema objetivo. En la figura siguiente se muestra un diagrama del protocolo TCP de tres vías, conocido como *three-way handshake*.



Exploración TCP SYN. Esta técnica es conocida como exploración semiabierta debido a que no se realiza una conexión TCP completa. Por el contrario, se envía un paquete SYN al puerto objetivo. Si se recibe un SYN/ACK de este puerto, podemos deducir que está en el estado LISTENING. Si se recibe un RST/ACK, querrá decir, normalmente, que el puerto no está a la escucha. El sistema que está llevando a cabo la exploración de puertos enviará un RST/ACK para que no se establezca nunca una conexión completa. Esta técnica tiene la ventaja de ser más cautelosa que una conexión TCP completa, y puede no ser detectada por el sistema objetivo.

Exploración TCP FIN. Esta técnica envía un paquete FIN al puerto objetivo. Basándose en RFC 793 (que especifica la operación de TCP), el sistema objetivo debería devolver un RST para todos los puertos que se encuentren cerrados. Esta técnica normalmente sólo funciona en stack TCP/IP basado en UNIX.

Exploración árbol de Navidad TCP. Esta técnica envía paquetes FIN, URG y PUSH al puerto objetivo. Basándose en RFC 793, el sistema objetivo debería devolver un RST para todos los puertos cerrados.

Exploración nula TCP. Esta técnica apaga todas las banderas (flags). Basándose en RFC 793, el sistema objetivo debería devolver un RST para todos los puertos cerrados.

Exploración UDP. Esta técnica envía un paquete UDP al puerto objetivo. Si el puerto responde con un mensaje similar a "puerto ICMP no alcanzable", el puerto está cerrado. Por el contrario, si no se recibe ese mensaje, se puede deducir que el puerto está abierto. Dado que UDP es conocido como un protocolo sin conexión, la confiabilidad de esta técnica depende en gran medida de muchos factores relacionados con la utilización de los recursos del sistema y de red. Además, la exploración UDP es un proceso muy lento si se intenta analizar un dispositivo que utilice filtrado pesado de paquetes.

Ciertos equipos devuelven paquetes RST para todos los puertos que se hayan explorado, estén o no a la escucha. Por tanto, los resultados obtenidos pueden variar según la máquina que se escanea.

Con independencia de la herramienta y la técnica utilizada, con el escaneo se está intentando identificar los puertos abiertos, lo que proporciona signos indicativos del sistema operativo. Por ejemplo, cuando los puertos abiertos son el 135 y el 139, hay grandes probabilidades de que el sistema operativo objetivo sea Windows NT/2000. Eso se debe a que Windows NT/2000, normalmente, escucha por los puertos 135 y 139, lo cual lo diferencia de Windows 95/98, que tan sólo escucha por el puerto 139.

Los números de puerto por debajo de 1024 se llaman puertos bien conocidos (*well-known ports*) y se reservan para servicios estándar. Por ejemplo, HTTP usa el puerto 80 y DNS el puerto 25. La lista de puertos bien conocidos se da en el RFC 1700.

Algunos de los puertos más comunes y los servicios que se ejecutan sobre ellos son los siguientes:

- 20/21 FTP (File Transfer Protocol). Utilizado para intercambiar archivos con máquinas remotas. El puerto 20 se usa para control de la conexión y el puerto 21 para los datos en sí.
- 23 Telnet. Proporciona una conexión de terminal a un sistema remoto.
- 25 SMTP. Se encarga de enviar y almacenar correo electrónico.
- 53 DNS. Sistema de nombre de dominio.
- 80 HTTP. El World Wide Web (telaraña mundial).
- 110 POP3. Acceso remoto al correo electrónico.
- 143 IMAP. Otro método de acceso remoto al correo electrónico.
- 161 SNMP. Sistema de gestión de red simple

Los *puertos registrados* van desde 1024 hasta 49151 y están ligados a los servicios que prestan las aplicaciones. Los *puertos privados* van desde 49152 hasta 55535. En teoría ningún servicio debería ser asignado a dichos puertos. Son muy usados por los troyanos.

Si mediante *netstat –an* aparecen puertos altos en escucha, puede ser que haya un troyano corriendo, tal como SubSeven, NetBus o Back Orifice. Por ejemplo, SubSeven usa típicamente el puerto 6667 TCP. Estos programas instalan, sin conocimiento del usuario, un módulo servidor que envía contraseñas y otros datos de interés al atacante, abriendo un puerto en la PC de la víctima.

Cuando se activa la opción compartir archivos en la red Microsoft con NetBIOS, se abren eventualmente los puertos TCP 137 (NetBIOS Name Service), 138 (NetBIOS Datagram Service) y 139 (NetBIOS Session Service) y los puertos UDP 1027-1029.

Los sistemas de mensajería instantánea (IM) utilizan los siguientes puertos, pero que pueden a veces variar:

- MSN Messenger: TCP 1503, 1863, 6891; UDP 13324, 13325
- Yahoo Messenger TCP 5010
- AOL: TCP 5190, 4433

Netmeeting utiliza los puertos TCP 1720 y 1503.

Si aparece abierto el puerto 5000 en Windows ME/XP, se debe a que está activo *ssdpsrv.exe*, el cual es utilizado para ciertas funciones plug & play (compruébelo mediante *msconfig*).

En conclusión, mediante una sencilla exploración de puertos TCP y UDP se pueden hacer suposiciones sobre la vulnerabilidad de los sistemas. Por ejemplo, si un servidor Windows NT/2000 tiene abierto el puerto 139, se estará corriendo un gran riesgo, a menos que se tomen las contramedidas adecuadas para proteger el acceso a ese puerto. Por el contrario, es virtualmente imposible comprometer la seguridad de un servicio remoto si no está a la escucha. Por tanto, es importante recordar que cuantos más servicios se estén ejecutando, mayor será la probabilidad de comprometer el sistema.

Recientemente se ha publicado un interesante artículo sobre el escaneo de puertos por parte de gusanos en Internet. Sus autores monitorearon los intentos de propagación tres variantes de redCode y dos variantes de Nimda. Los resultados son impresionantes. Habiendo analizado las conexiones en una red que se corresponde con el 1/256 del espacio de direcciones de Internet, se observaron más de 2.500 millones de intentos de conexión, con picos de 2000 intentos por segundo. Extrapolando esos datos a todo Internet, habría unos 6.4 billones (un billón es un millón de millones) de intentos de conexión, con un tráfico de unos 60 terabytes.

Aún sin contar la contaminación en sí de otras máquinas, que genera un tráfico extra importante, el simple escaneo de direcciones IP a la caza de servidores web (que pueden ser vulnerables o no), consume una cantidad de recursos impresionante.

Algunas de las conclusiones de este trabajo son:

- Una máquina anónima conectada a Internet experimentará un escaneo por parte de alguno de esos gusanos cada hora, aproximadamente.
- En una red con 256 direcciones públicas (una clase C estándar), se recibe un escaneo cada 14 segundos.
- El no tener una IP oficial o publicada en un DNS no ofrece ninguna protección, ya que estos escaneos se realizan de forma aleatoria sobre el espacio de direcciones IP.
- Por lo tanto, una máquina que no esté protegida y bien configurada NO debe conectarse a Internet hasta que se asegure convenientemente.

A continuación se va a describir una serie de herramientas a fin de que las utilice para escaneo de puertos, detección de vulnerabilidades y pruebas de penetración.

El sistema operativo Windows 98/ME no es particularmente apto para realizar este tipo de pruebas debido a que su stack TCP/IP no permite utilizar lo que se conoce como *raw sockets*, por lo que la mayoría de los productos más poderosos se consiguen para Windows NT/2000/XP y Linux.

Empiece con LANguard y Shadow Security Scanner y luego continúe con ISS, Retina, CyberCop y Nmap. Si está familiarizado con Linux, puede utilizar algunas de las herramientas que existen para esa plataforma (por ejemplo, Sara, Nessus, Cheops, Saint) o un CD Live que se corre directamente desde un CD-ROM.

Como blanco u objetivo para las pruebas, utilice su máquina y luego otra en su misma red o en Internet. Capture el tráfico mediante un sniffer como Iris, Ethereal o Agilent Advisor para así entender mejor cómo trabajan y qué técnicas de exploración de puertos utilizan.

Fase 3.1: LANguard

LANguard es un producto desarrollado por GFI Software Ltd. (*http://www.gfi.com*) que se caracteriza por ser muy amigable y trabajar bien sobre todas las plataformas Windows, incluyendo Windows 98/ME.

Fase 3.2: Shadow Security Scanner

SSS es un producto desarrollado por Safety Lab (*http://www.safety-lab.com*) que se caracteriza por ser muy rápido y trabajar bien sobre todas las plataformas Windows.

Arranque SSS desde Windows mediante *Inicio Programas*. Si el período de prueba de 15 días ha caducado, no sirve de nada atrasar la fecha del computador. Nota: esta forma de registro es sólo para fines didácticos y no para uso personal o comercial.

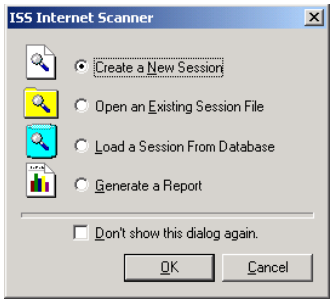
Finalmente proceda a hacer las pruebas sobre el blanco. Si el programa se pone muy pesado, disminuya el número de *threads* y si no responde, finalice la tarea mediante *Alt-Control-Del*.

Fase 3.3: Internet Security Scanner (ISS)

Instale ISS en una máquina con sistema operativo Windows NT/2000/XP.

Corra Internet Scanner desde Windows 2000/XP mediante *Inicio* | *Programas* | *Internet Scanner*

En la ventana inicial que aparece, seleccione *Create a New Session*.



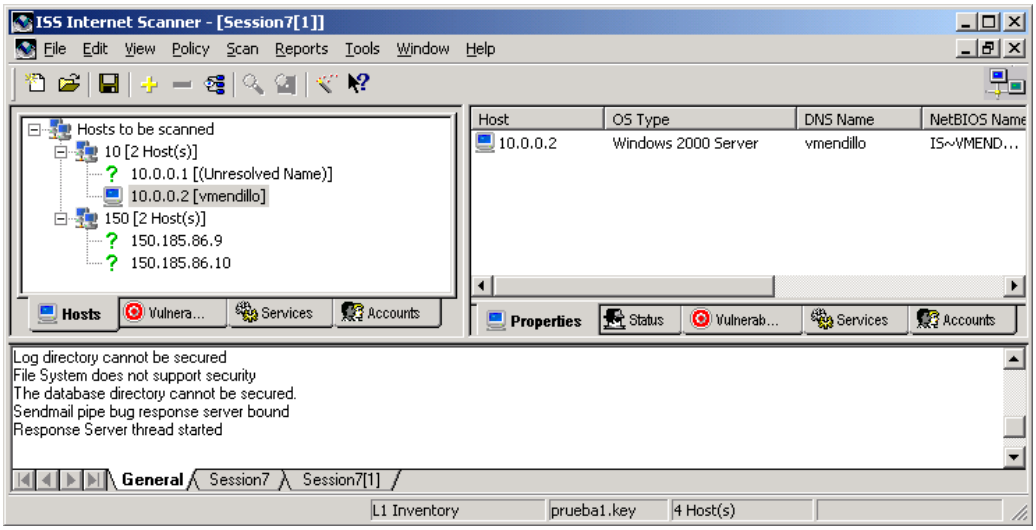
En la ventana *Select a Key*, pulse *Display key* y vea las características de la clave a utilizar. Luego pulse *Next.*

En la ventana *Select A policy*, seleccione una política apropiada al sistema que va a evaluar. Se recomienda empezar con *L1 Inventory*.

En la ventana *Specify host*, seleccione *Ping valid hosts in your key*.

En la ventana *Set Host Ping Range*, coloque la gama de direcciones IP de la red que desea explorar (por ejemplo, 10.0.0.1-10.0.0.254. También se pueden poner 2 o más gamas de direcciones, por ejemplo, 10.0.0.1-10.0.0.63, 200.44.32.12-200.44.32.28

Si todo está bien, debería aparecer la ventana de ISS e inmediatamente arrancar el descubrimiento de la red seleccionada.



Ventana principal de ISS

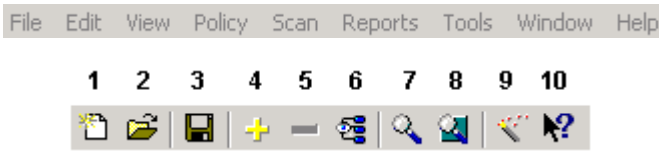
La ventana principal de ISS está dividida en 3 sub-ventanas llamadas vistas (*views*).

- La vista izquierda muestra la red y sus componentes en forma de árbol.
- La vista derecha muestra la lista de la direcciones IP y sus detalles.
- La vista inferior muestra información de estado a medida que procede el escaneo.

Haga clic sobre la pestaña *General* al fondo de la pantalla. En la vista de estado se alerta sobre algunas vulnerabilidades encontradas en su PC y otras noticias.

Haga clic sobre la pestaña *Session1* al fondo de la pantalla para analizar la sesión en curso.

En la vista izquierda haga clic sobre el host que corresponde a su PC y a continuación empiece el escaneo de ese host pulsando el botón 7 en la barra de tareas (o seleccione *Scan* → *Scan Now*) en el menú.



Menú y barra de herramientas

Seleccionando una de las 4 pestañas (*tabs*) se detalla la información de distintos modos.

Modos de visualización

Hosts: muestra la lista de las máquinas que van a ser escaneadas (o que han sido escaneadas). Haciendo clic sobre un host aparecen más pestañas con opciones en la ventana a la derecha. Mediante los botones 4 y 5 se pueden añadir o quitar máquinas. También se puede hacer mediante *Edit* → *Add host* y *Edit* → *Remove host.*

Vulnerabilities: muestra las vulnerabilidades detectadas por ISS. Haciendo clic sobre el sígno + de una vulnerabilidad, se muestran cuáles hosts han sido encontrados vulnerables. Haciendo clic con el botón derecho se explica en detalle la vulnerabilidad.

Services: muestra los servicios que están corriendo sobre el host.

Accounts: muestra la cuentas de usuarios, de grupo y de máquinas descubiertas.

La vista a la derecha posee 5 pestañas que detallan la información sobre un determinado host.

Información sobre el host

Haga clic sobre cada una de las pestañas y analice la información desplegada. Note en particular los servicios activos y los puertos abiertos.

La columna *OS Type* bajo *Properties* es muy importante, ya que muestra el sistema operativo que utiliza la máquina (por ejemplo, Windows NT). La forma de averiguarlo es muy ingeniosa pero no siempre es precisa.

Antes de continuar las pruebas, se recomienda actualizar la base de datos de vulnerabilidades mediante *Inicio* | *Programas* | *Internet Scanner* | *X-Press Update Install.* Seleccione *LocalDrive or Network Share* y navegue a la carpeta *Vulnerabilidades* | *Iris* | *Xpress Updates.*

Luego de haber hecho esta primera actualización, puede realizar una actualización todavía más reciente seleccionando *Web Server* en lugar de *LocalDrive or Network Share.*

Nota: Estos 2 procesos llevan bastante tiempo, así que los puede posponer para otra oportunidad.

Fase 3.4: Retina

Instale Retina en una máquina con sistema operativo Windows NT/2000/XP y proceda a hacer pruebas sobre el blanco.

Retina es un un verificador de seguridad automatizado para servidores conectados a Internet, intranets y extranets, desarrollado por eEye Digital Security Team (http://www.eEye.com)

En el vertiginoso mundo de la seguridad de redes, los administradores de sistemas suelen partir en desventaja. Los ataques a la seguridad de equipos conectados a Internet cambian continuamente y se basan en conocer antes que nadie las fallas de seguridad de nuevos programas y versiones. Sin embargo, con el auxilio de una aplicación como Retina, el panorama cambia radicalmente.

Retina es como un auditor de seguridad. El administrador sólo debe instalarlo y empezar a activar exploraciones sobre direcciones IP. Basta con conocer la IP del propio equipo (o usar la dirección del loopback), o bien de otro equipo local, para iniciar el análisis. Retina explorará de forma exhaustiva la configuración de todos los servicios activos, detectando inmediatamente problemas y avisando sobre el potencial peligro de algunas configuraciones defectuosas.

Retina incide con especial atención en la facilidad de uso. Su configuración no requiere manipular montones de parámetros al alcance sólo de usuarios avanzados; por el contrario, se automatiza al máximo la exploración, de modo que el usuario, al finalizar ésta, cuente en pantalla con un máximo de información sencilla y bien distribuida para tomar las medidas necesarias. El programa está enlazado internamente con las bases de datos mantenidas constantemente

al día por el fabricante en su sede Web, y gracias a ello diagnosticar un problema y encontrar la forma de resolverlo (cambiar el registro, instalar un parche...) normalmente se lleva a cabo en cuestión de minutos.

El motor de automatización de Retina es capaz de activar alertas mediante cuadros de diálogo locales, mensajes a una cuenta de correo o a través de Messenger. La funcionalidad del programador es limitada: sólo se puede configurar para activarse en días concretos de la semana y únicamente admite horas en punto. No es posible, por ejemplo, configurar un análisis el día 1 de cada mes a las 8:30h.

Debido a su cometido, Retina requiere una actualización constante. La característica *Auto Update* garantiza una actualización sin problemas en cualquier momento, con una simple conexión al sede web de eEye.

La estructura funcional de Retina se basa en el uso de módulos o componentes para acometer distintas tareas. Esta capacidad permite suavizar el proceso evolutivo de la aplicación en un futuro, apoyado en la publicación de una API para facilitar la programación de nuevos extras por parte de terceros. Actualmente, Retina utiliza cuatro componentes:

- Scanner: se trata del componente central de Retina, y es el responsable de auditar la seguridad de la red. Su propósito es rastrear las direcciones IP indicadas por el usuario (puntuales o rangos) y comprobar todos los puertos abiertos de acuerdo con el perfil en uso. El escáner es capaz de detectar el protocolo utilizado por cada puerto comprobado, de modo que no es ningún problema que el equipo utilice puertos no estándar para determinados servicios.
- Miner: es un módulo que explora activamente la red en busca de brechas de seguridad. Para ello utiliza un motor de inteligencia artificial que le permite emular los mecanismos utilizados más comúnmente por los hackers.
- Tracer: este módulo crea un traceroute (ruta de paso) entre el equipo local y un equipo de destino. En la ruta se incluyen los tiempos de respuesta, y los resultados se muestran en forma de gráfico.
- Browser: convierte la interfaz de Retina en un navegador web convencional, pero con el añadido de un panel de detalles, que lista los enlaces a equipos externos de la página, y otro con información sobre el archivo que contiene la página visualizada.

Fase 3.5: Nmap

Nmap fue desarrollado por un joven programador ruso de apodo Fyodor, para facilitar el escaneo de grandes redes a fin de determinar qué servidores se encuentran activos y qué servicios ofrecen.

Nmap permite un gran número de técnicas de escaneo como: UDP, TCP connect(), TCP SYN (half open), ftp proxy (bounce attack), Reverse-ident, ICMP (ping sweep), FIN, ACK sweep, Xmas Tree, SYN sweep y Null scan. Además proporciona características avanzadas como la detección remota del sistema operativo por medio de huellas TCP/IP, escaneo tipo stealth (oculto), retraso dinámico y cálculos de retransmisión, escaneo paralelo, detección de servidores inactivos por medio de pings paralelos, escaneo con señuelos, detección de filtrado de puertos, escaneo por fragmentación y especificación flexible de destino y puerto.

Nmap se ha vuelto muy popular en el mundo de la seguridad informática y hasta ha aparecido en el cine. En la película *The Matrix Reloaded* (la secuela de *The Matrix*), por una vez el séptimo arte presenta de forma más fiel cómo los hackers desarrollan sus actividades, utilizando herramientas reales como Nmap. La escena es muy breve, unos pocos segundos, pero suficientes para reconstruirlos. Trinity, la atractiva superhacker, desde una sesión *root* en una máquina Unix (identificable por el prompt #), utiliza Nmap 2.54 BETA25 para identificar los servicios que ofrece la máquina 10.2.2.2. Encuentra el puerto 22/tcp, correctamente identificado como SSH. A continuación, utiliza un programa llamado sshnuke que muestra este texto "Attempting to exploit SSHv1 CRC32". Se trata de un exploit que le permite cambiar la contraseña del usuario root del sistema remoto. Si bien no se tiene constancia de la existencia de ningún exploit llamado "sshnuke", lo que si es real es la vulnerabilidad y también los efectos de la misma. La utilización de esta vulnerabilidad permite obtener privilegios de root en el sistema remoto.

Si usted es una persona impaciente, puede pasar directamente a la sección de ejemplos más adelante, donde encontrará casos de uso más corrientes. Para aprender a usar Nmap a fondo, consulte *Nmap –h* desde una ventana de comandos para así ver un listado de todas las opciones.

Tipos de Escaneo

Nmap -sT

Escaneo TCP connect(): Es la forma más básica de escaneo TCP. La llamada de sistema connect() proporcionada por el sistema operativo se usa para establecer una conexión con todos los puertos interesantes de la máquina. Si el puerto está a la escucha, connect() tendrá éxito, de otro modo, el puerto resulta inalcanzable. Este tipo de escaneo resulta fácilmente detectable dado que los registros de la máquina de destino muestran un montón de conexiones y mensajes de error para aquellos servicios que aceptan la conexión para luego cerrarla inmediatamente.

Nmap -sS

Escaneo TCP SYN: A menudo se denomina a esta técnica escaneo "half open" (medio abierto), porque no se abre una conexión TCP completa. Se envía un paquete SYN, como si se

fuese a abrir una conexión real y se espera que llegue una respuesta. Un SYN|ACK indica que el puerto está a la escucha. Un RST es indicativo de que el puerto no está a la escucha. Si se recibe un SYN|ACK, se envía un RST inmediatamente para cortar la conexión (en realidad es el kernel del sistema operativo el que hace esto). La ventaja principal de esta técnica de escaneo es que será registrada por muchos menos máquinas de destino que la anterior.

Nmap -sF -sX -sN
Modos Stealth FIN, Xmas Tree o Null scan: A veces ni siquiera el escaneo SYN resulta lo suficientemente clandestino. Algunas firewalls y filtros de paquetes vigilan el envío de paquetes SYN a puertos restringidos, y programas disponibles como Synlogger y Courtney detectan este tipo de escaneo. Estos tipos de escaneo avanzado, sin embargo, pueden cruzar estas barreras sin ser detectados. La idea es que se requiere que los puertos cerrados respondan a nuestro paquete de prueba con un RST, mientras que los puertos abiertos deben ignorar los paquetes en cuestión (véase RFC 794 pp 64). El escaneo FIN utiliza un paquete FIN vacío como prueba, mientras que el escaneo Xmas tree activa las flags FIN, URG y PUSH. El escaneo NULL desactiva todas las flags. Por desgracia Microsoft (como de costumbre) decidió ignorar el estándar completamente y hacer las cosas a su manera. Debido a esto, este tipo de escaneo no funcionará con sistemas basados en Windows. En el lado positivo, esta es una buena manera de distinguir entre las dos plataformas. Si el escaneo encuentra puertos cerrados, probablemente se trate de una máquina Unix, mientras que todos los puertos abiertos es indicativo de Windows. Excepcionalmente, Cisco, BSDI, HP/UX, MVS, y IRIX también envían RST en vez de desechar el paquete.

Nmap -sP
Escaneo ping: A veces únicamente se necesita saber qué servidores en una red se encuentran activos. Nmap puede hacer esto enviando peticiones de respuesta ICMP a cada dirección IP de la red que se especifica. Aquellos servidores que responden se encuentran activos. Desafortunadamente, algunos sitios web como microsoft.com bloquean este tipo de paquetes. Nmap puede enviar también un paquete TCP ACK al puerto 80 (por defecto). Si se obtiene por respuesta un RST, esa máquina está activa. Una tercera técnica implica el envío de un paquete SYN y la espera de un RST o un SYN/ACK. Por defecto, Nmap usa las técnicas ICMP y ACK en paralelo. Se puede cambiar la opción -p descrita más adelante. Nótese que el envio de pings se realiza por defecto de todas maneras y que sólamente se escanean aquellos servidores de los que se obtiene respuesta. Use esta opción solamente en el caso de que desee un ping sweep (barrido ping) sin hacer ningún tipo de escaneo de puertos.

Nmap -sU
Escaneo UDP: Este método se usa para saber qué puertos UDP (Protocolo de Datagrama de Usuario, RFC 768) están abiertos en un servidor. La técnica consiste en enviar paquetes UCP de 0 bytes a cada puerto de la máquina objetivo. Si se recibe un mensaje ICMP de puerto no alcanzable, entonces el puerto está cerrado. De lo contrario, asumimos que está abierto. Algunos expertos piensan que el escaneo UDP no tiene sentido, pero basta recordar el agujero Solaris rcpbind. Puede encontrarse a rcpbind escondido en un puerto UDP no documentado en algún lugar por encima del 32770. Por lo tanto, no importa que el 111 esté bloqueado por la firewall.

¿Quién puede decir en cual de los más de 30000 puertos altos se encuentra a la escucha el programa? ¡Con un escáner UDP se puede! Tenemos también el programa de puerta trasera Back Orifice que se oculta en un puerto UDP configurable en las máquinas Windows, por no mencionar los muchos servicios frecuentemente vulnerables que usan UDP como snmp, tftp, NFS, etc. Por desgracia, el escaneo UDP resulta a veces tremendamente lento debido a que la mayoría de los servidores implementan una sugerencia recogida en el RFC 1812 (sección 4.3.2.8) acerca de la limitación de la frecuencia de mensajes de error ICMP. Por ejemplo, el kernel de Linux (en /ipv4/icmp.h) limita la generación de mensajes de destino inalcanzable a 80 cada cuatro segundos, con una penalización de 1/4 de segundo si se rebasa dicha cantidad. Solaris tiene unos límites mucho más estrictos (más o menos 2 mensajes por segundo) y por lo tanto lleva más tiempo hacerle un escaneo. Nmap detecta este límite de frecuencia y se ralentiza en consecuencia, en vez de desbordar la red con paquetes inútiles que la máquina destino ignorará. Como de costumbre, Microsoft ignoró esta sugerencia del RFC y no parece que haya previsto ningún tipo de límite de frecuencia para las máquinas Windows. Debido a esto resulta posible escanear los 65K puertos de una máquina Windows muy rápidamente.

Opciones Generales
No se requiere ninguna, pero algunas de ellas que se describen a continuación pueden resultar de gran utilidad.

Nmap -P0
No intenta hacer ping a un servidor antes de escanearlo. Esto permite el escaneo de redes que no permiten que pasen peticiones (o respuestas) de ecos ICMP a través de su firewall. Microsoft.com es un ejemplo de una red de este tipo, y, por lo tanto, debería usarse siempre Nmap -P0 o Nmap -PT80 al escanear microsoft.com.

Nmap -PT
Usa el ping TCP para determinar qué servidores están activos. En vez de enviar paquetes de petición de ecos ICMP y esperar una respuesta, se lanzan paquetes TCP ACK a través de la red de destino (o a una sola máquina) y luego se espera a que lleguen las respuestas. Los servidores activos responden con un RST. Esta opción mantiene la eficiencia de escanear únicamente aquellos servidores que se encuentran activos y la combina con la posibilidad de escanear redes/servidores que bloquean los paquetes ping. Para establecer el puerto de destino de los paquetes de prueba usar -PT <número de puerto). El puerto por defecto es el 80, dado que normalmente este puerto no es un puerto filtrado.

Nmap -PS
Esta opción usa paquetes SYN (petición de conexión) en vez de los paquetes ACK. Los servidores activos deberían responder con un RST (o, en raras ocasiones, un SYN|ACK).

Nmap -PI

Esta opción usa un paquete ping (petición de eco ICMP) verdadero. Encuentra servidores que están activos y también busca direcciones de broadcast dirigidas a subredes en una red. Se trata de direcciones IP alcanzables desde el exterior que envían los paquetes IP entrantes a una subred de servidores. Estas direcciones deberían eliminarse, si se encontrase alguna, dado que suponen un riesgo elevado ante numerosos ataques de negación de servicio (el más corriente es Smurf).

Nmap -PB
Este es el tipo de ping por defecto. Usa los barridos ACK (Nmap -PT) e ICMP (Nmap -PI) en paralelo. De este modo se pueden alcanzar firewalls que filtren uno de los dos (pero no ambos).

Nmap -O
Esta opción activa la detección remota del sistema operativo por medio de la huella TCP/IP. En otras palabras, usa un conjunto de técnicas para detectar sutilezas en la pila de red subyacente del sistema operativo de los servidores que se escanean. Usa esta información para crear una 'huella' que luego compara con una base de datos de huellas de sistemas operativos conocidas (el archivo nmap-os-fingerprints) para decidir qué tipo de sistema se está escaneando.

Nmap -I
Esta opción activa el escaneo TCP de identificación contraria. Tal y como comenta Dave Goldsmith en un correo Bugtraq de 1996, el protocolo ident (RFC 1413) permite la revelación del nombre del usuario propietario de cualquier proceso conectado vía TCP, incluso aunque ese proceso no haya iniciado la conexión. De este modo se puede, por ejemplo, conectar con el puerto http y luego usar identd para descubrir si el servidor está ejecutándose como root. Esto sólo se puede hacer con una conexión TCP completa con el puerto de destino (o sea, la opción de escaneo -sT). Cuando se usa Nmap -I, se consulta al identd del servidor remoto sobre cada uno de los puertos abiertos encontrados en el sistema. Por supuesto, esto no funcionará si el servidor en cuestión no está ejecutando identd.

Nmap -F
Esta opción hace que el escaneo solicitado de tipo SYN, FIN, XMAS, o NULL usando pequeños paquetes IP fragmentados. La idea consiste en dividir la cabecera TCP en varios paquetes para ponérselo más difícil a los filtros de paquetes, sistemas de detección de intrusión y otras inconveniencias por el estilo que tratan de saber lo uno está haciendo. ¡Tenga cuidado con esto! Algunos programas tienen problemas a la hora de manejar estos paquetes tan pequeños. Aunque este método no podrá con filtros de paquetes y firewalls que ponen en cola todos los fragmentos IP (como en el caso de la opción CONFIG_IP_ALWAYS_DEFRAG en la configuración del kernel de Linux), también es verdad que algunas redes no pueden permitirse el efecto negativo que esta opción causa sobre su rendimiento y por lo tanto la dejan desactivada. Esta opción no funciona con todos los sistemas. Funciona bien con sistemas Linux, FreeBSD y OpenBSD y algunas personas han informado de éxitos con otras variantes Unix.

Nmap -v
Modo de información ampliada. Esta opción resulta muy recomendable y proporciona gran cantidad de información sobre lo que está sucediendo. Se puede usarla dos veces para un efecto mayor.

Nmap -h
Esta opción tan práctica muestra una pantalla de referencia rápida sobre las opciones de uso de Nmap.

Nmap -o <nombre_de_archivo_de_registro>
Esta opción guarda los resultados de los escaneos en forma humanamente inteligible en el archivo especificado como argumento.

Nmap -m <nombre_de_archivo_de_registro>
Esta opción guarda los resultados de los escaneos en un formato comprensible para una máquina en el archivo especificado como argumento.

Nmap -i <nombre_de_archivo_de_entrada>
Lee especificaciones de servidores o redes de destino a partir del archivo especificado en vez de hacerlo de la línea de comandos. El archivo debe contener una lista de expresiones de servidores o redes separadas por espacios, tabuladores o nuevas líneas. Use un guión (-) como nombre_de_archivo_de_entrada si desea que Nmap tome las expresiones de servidores de stdin. Véase la sección Especificación de Objetivo para más información sobre expresiones con las que poder completar este archivo.

Nmap -p <rango de puertos>
Esta opción determina los puertos que se quieren especificar. Por ejemplo, '-p 23' probará solo el puerto 23 del servidor(es) objetivo. '-20-30,139,60000-' escanea los puertos del 20 al 30, el puerto 139 y todos los puertos por encima de 60000. Por defecto se escanean todos los puertos entre el 1 y el 1024 así como los que figuran en el archivo /etc/services.

Nmap -F
Modo de escaneo rápido. Implica que sólo se desean escanear aquellos puertos que figuran en /etc/services. Obviamente esto resulta mucho más rápido que escanear cada uno de los 65535 puertos de un servidor.

Nmap -D <señuelo1 [,señuelo2][,ME],...>
Especifica que se desea efectuar un escaneo con señuelos, el cual hace que el servidor escaneado piense que la red destino del escaneo está siendo escaneada también por los servidores especificados como señuelos. Así, sus IDs pueden informar de entre 5 y 10 escaneos procedentes de direcciones IP únicas, pero no sabrán que dirección IP les estaba escaneando realmente y cúales eran señuelos inocentes. Separe cada servidor señuelo con comas, y puede usar opcionalmente 'ME' como señuelo que representa la posición que quiere que ocupe su dirección IP. Si coloca 'ME' en la sexta posición o superior, es muy poco probable que algunos escáneres de puertos comunes (como el excelente scanlogd de Solar Designer) lleguen incluso a mostrar su dirección IP. Si no se usa 'ME', Nmap le colocará a usted en una posición aleatoria. Nótese que aquellos servidores usados como señuelos deben encontrarse

activos, o, de lo contrario podría provocar un desbordamiento (flood) SYN en su objetivo. Por otra parte, resultará bastante fácil saber qué servidor está escaneando si únicamente hay uno activo en la red. Nótese también que algunos detectores de escáneres de puertos opondrán un firewall o bien negarán el enrutamiento a aquellos servidores que intenten escanear sus puertos. De este modo se podría provocar inadvertidamente que la máquina que se está intentando escanear perdiese contacto con los servidores usados como señuelos. Esto podría causarles a los servidores escaneados verdaderos problemas si los servidores señuelo fuesen, por ejemplo, su gateway a Internet o incluso "localhost". Debería usarse esta opción con extremo cuidado. La verdadera moraleja de este asunto es que un detector de escaneos de puertos que aparenten tener intenciones poco amistosas no debería llevar a cabo acción alguna contra la máquina que aparentemente le está escaneando. ¡Podría no ser más que un señuelo! Los señuelos se usan tanto en el escaneo ping inicial (usando ICMP, SYN, ACK, o lo que sea) como en la fase de escaneo de puertos propiamente dicha. También se usan los señuelos en la fase de detección remota del sistema operativo (Nmap -O). Vale la pena destacar que el uso de demasiados señuelos puede ralentizar el proceso de escaneo y, potencialmente, hacer que sea menos exacto. Por otra parte, algunos ISPs filtrarán los paquetes manipulados y los desecharán, aunque muchos (actualmente la mayoría) no ponen restricciones a este tipo de paquetes.

Nmap -S <Dirección_IP>
En determinadas circunstancias, es posible que no sea capaz de determinar la dirección IP de origen (se lo hará saber si éste es el caso). En este caso, use -S con su dirección IP (de la interfaz a través del cual desea enviar los paquetes). Otro posible uso de esta opción es el de manipular el escaneo para hacer creer a los servidores de destino que Nmap alguien más les está escaneando. ¡Imagínese a una compañía escaneada repetidamente por una compañía rival! Esta no es la función para la que se ha diseñado esta opción (ni su propósito principal). Simplemente revela una posibilidad que la gente debería tener en cuenta antes de acusar a los demás de escanear sus puertos. La opción Nmap -e será necesaria en general para este tipo de uso.

Nmap -e <interfaz>
Le dice a Nmap qué interfaz ha de usar para enviar y recibir paquetes. El programa debería detectar esto por sí mismo, pero le informará si no es así.

Nmap -g <número_de_puerto>
Establece el número de puerto de origen a usar en los escaneos. Muchas instalaciones de firewalls y filtros de paquetes inocentes hacen una excepción en sus reglas para permitir que las atraviesen y establezcan una conexión paquetes DNS (53) o FTP-DATA (20). Evidentemente esto contraviene completamente las ventajas en materia de seguridad que comporta un firewall dado que los intrusos pueden enmascararse como DNS o FTP con una simple modificación de su puerto de origen. Por supuesto, debería probarse primero con el puerto 53 para un escaneo UDP y los escaneos TCP deberían probar el 20 antes del 53. Nótese que el uso de esta opción penaliza levemente el rendimiento del escaneo, porque a veces se almacena información útil en el número de puerto de origen.

N**map -M <max sockets>**
Establece el número máximo de sockets que se usarán en paralelo para un escaneo TCP connect() (escaneo por defecto). Resulta útil a la hora de ralentizar ligeramente el proceso de escaneo con el fin de evitar que la máquina de destino se cuelgue. Otra manera de hacerlo es usar -sS, que normalmente les resulta más fácil de asumir a las máquinas de destino.

Nmap Especificación de Objetivo
Cualquier cosa que no es una opción (o el argumento de una opción) en Namp se trata como una especificación de servidor de destino. El caso más simple consiste en especificar servidores aislados o direcciones IP en la línea de comandos. Si pretende escanear una subred de direcciones IP, entonces se puede añadir Nmap '/mask' a la dirección IP o al nombre del servidor. Nmap mask debe estar entre 0 (escanea toda Internet) y 32 (escanea únicamente el servidor especificado). Use /24 para escanear una dirección de clase 'C' y /16 para la clase 'B'. Nmap dispone también de una notación mucho más potente que permite la especificación de direcciones IP usando listas/rangos para cada elemento. De este modo, se puede escanear la red de clase 'B' completa 128.210.*.* especificando '128.210.*.*' o '128.210.0 - 255.0-255' o incluso '128.210.1 - 50,51 - 255.1,2,3,4,5 - 255'. Y, por supuesto, se puede usar la notación de máscara: '128.210.0.0/16'. Todas ellas son equivalentes. Si se usan asteriscos ('*'), ha de tenerse en cuenta que la mayoría de los shells requieren que se salga de ellos con caracteres / o que se les proteja con comillas. Otra posibilidad interesante consiste en dividir Internet en el otro sentido. En vez de escanear todos los servidores en una clase 'B', se puede escanear '*.*.5.6-7' para escanear todas las direcciones IP terminadas en .5.6 o .5.7 Escoja sus propios números. Para más información sobre la especificación de servidores a escanear, véase la sección de ejemplos a continuación.

Ejemplos
A continuación se muestran algunos ejemplos del uso de Nmap que abarcan desde los usos más normales y frecuentes a los más complejos o incluso esotéricos. Nótese que se han incluido direcciones IP y nombres de dominio reales para hacer las cosas más concretas. Usted debería sustituirlos por números y direcciones de su propia red.

Nmap -v objetivo.ejemplo.com
Esta opción escanea todos los puertos TCP reservados en la máquina objetivo.ejemplo.com. La -v implica la activación del modo de información ampliada.

Nmap -sS -O objetivo.ejemplo.com/24
Lanza un escaneo SYN oculto contra cada una de las máquinas activas de las 255 máquinas de la clase 'C' donde se aloja objetivo.ejemplo.com. También trata de determinar el sistema operativo usado en cada una de las máquinas activas.

Nmap -sX -p 22,53,110,143 "128.210.*.1-127"
Envía un escaneo Xmas tree a la primera mitad de cada una de las 255 posibles subredes de 8 bits en el espacio de direcciones

clase 'B' 128.210. Se trata de comprobar si los sistemas ejecutan sshd, DNS, pop3d, imapd o el puerto 4564. Nótese que el escaneo Xmas no funciona contra servidores ejecutando cualquier sistema operativo de Microsoft debido a una pila TCP deficiente. Lo mismo se aplica a los sistemas CISCO, IRIX, HP/UX, y BSDI.

Nmap -v -p 80 '*.*.2.3-5'
En vez de centrarse en un rango específico de direcciones IP, resulta a veces interesante dividir Internet en porciones y escanear una pequeña muestra de cada porción. Este comando encuentra todos los servidores web en máquinas cuyas direcciones IP terminen en .2.3, .2.4, o .2.5. Se podría añadir también -sS. También encontrará máquinas mucho más interesantes si empieza en 127, así que es posible que desee usar '127-222' en vez del primer asterisco dado que esa sección tiene una densidad mucho mayor de máquinas interesantes (IMHO).

Fase 3.6: Linux

Existen versiones especializadas del sistema operativo Linux, con una gran cantidad de herramientas disponibles específicamente para verificar la seguridad informática y realizar pruebas de penetración. Claro está que se requiere un cierto conocimiento de Linux. Estas versiones se basan en distribuciones compactas de Linux ("Live CD") como Knoppix y Slax. El sistema se ejecuta directamente desde el CD-ROM, sin necesidad de isntalación, ya que existe soporte para una gran cantidad de dispositivos de hardware, que son detectados y configurados automáticamente.

Knoppix-STD (*Security Tools Distribution*) incluye sofisticadas herramientas agrupadas en varias categorías: encriptación (*gpg, openssl, stunnel*, etc.), firewalls (*shorewall*), honeypots (*honeyd, labrea*), detección de intrusos (*snort, aide*), analizador de tráfico y sniffers (*ethereal*), test de penetración, herramientas generales de red (*iptraf, ntop*). El listado completo se encuentra en *http://www.knoppix-std.org*. Por lo tanto, arrancando con este CD, se tiene un sistema Linux completamente usable, y con mas de 200 utilidades para administrar redes, analizarlas, monitorearlas, etc. Es ideal para auditores de seguridad.

BackTrack es un un Live CD que deriva de la fusión de otros dos populares Live CDs: *Whax* y *Auditor*. BackTrack no está basado en Knoppix, sino en Slackware, para facilitar la modularidad. Esto posibilita personalizarlo para incluir los módulos deseados, dependiendo de las necesidades. Tiene un gran repositorio de exploits y herramientas. Está pensado para auditores de seguridad y con este objetivo incluye una gran cantidad de exploits conocidos de sitios como: Securityfocus, Packetstorm, SecurityForest y Milw0rm. Se incluyen también las últimas versiones de las herramientas de seguridad por excelencia (*Nmap, Nessus, Metasploit Framework, Amap, Aireplay, Hydra*, etc.). Puede obtenerse en *http://new.remote-exploit.org*.

LocalAreaSecurity (L.A.S.) es otra distribución Live CD de pequeño tamaño (185 MB, pensado para instalarse en un CD pequeño, de la medida de una tarjeta de crédito). También está basado en Knoppix y utiliza el núcleo 2.4.20. Está especializado en la realización de pruebas de verificación de la seguridad y en las pruebas de penetración, incluyendo un gran número de herramientas: sniffers, cifrado, monitoreo de redes, detección de información oculta, obtención de información, etc. Puede obtenerse en *http://www.localareasecurity.com.*

Phlax (*Professional Hacker's Linux Assault Kit*) está especializado en la realización de análisis de seguridad, pruebas de penetración, análisis forense y auditores de seguridad. Incluye sniffers y herramientas para el análisis del tráfico capturado, herramientas para el análisis de protocolos y del funcionamiento del sistema, extracción de datos del sistemas de archivos, descifrado de archivos, etc. Puede obtenerse en *http://www.phlak.org.*

Fase 4: Análisis de vulnerabilidades y fallas encontradas

Una vez que se haya identificado el hardware, software, sistema operativo, parches, vulnerabilidades y otra información pertinente sobre la red, se debe investigar cómo se puede explotar todo eso para un posible ataque o penetración. Entre las fuentes de información se encuentran las siguientes listas:
bugtraq@netspace.org
firewalls@greatcircle.com
sneakers@cs.yale.edu
www-security@ns2.rutgers.edu
ntsecurity@iss

Además de pueden consultar los siguientes sitios:
www.cert.org
www.isc.org
www.kriptopolis.com
www.hispasec.com

Fase 5: Fase de ataques (pruebas de penetración y negación de servicio)

Llegado a este punto se está listo para empezar los ataques utilizando algunas de las herramientas descritas anteriormente u otras más específicas que existen en Internet. Algunos *Ataques* (*Denial_of_Service, WebCrack, NTexploits, SimpleTools*). Además se pueden aplicar nuevas técnicas en base a las vulnerabilidades específicas encontradas, tales como: contraseñas débiles, errores de configuración, bugs de software, buffer overflow, explotación de relación de confianza, etc.

También pueden probarse ataques de negación de servicio (DoS) con programas como ping of death, syn-flooder, dns killer, etc.

Los ataques deben dirigirse hacia cada una de las máquinas encontradas y que tengan servicios activos (ej. www, smtp, ftp, telnet, etc.).

Nota: Debe notificarse previamente al personal encargado de los equipos y sistemas a los cuales se van a efectuar estos ataques, a fin de que dé su autorización.

Fase 5.1: Pruebas desde Internet

Para evaluar la seguridad de una conexión a Internet no es indispensable recurrir a complejas técnicas o costosas herramientas. Una simple visita a los sitios web que se mencionan más adelante será útil para poner a prueba la seguridad. Estos sitios son realmente reveladores si se trabaja con un sistema operativo para servidor, como Windows 2000 o Linux. Sin embargo la mayoría de las pruebas no se podrán llevar a cabo si la máquina a evaluar está detrás de un firewall, un proxy o utiliza NAT (*Network Address Translation*) con direcciones internas no válidas (ej. 10.0.0.2).

- HacketWatch (*http://www.hackerwatch.org/safetyfirst*) realiza un test rápido para encontrar vulnerabilidades.
- La opción *Shields UP!* de Gibson Research (*http://grc.com/default.htm*) escanea las defensas y los puertos de su PC .
- *PC Flank* (*http://www.pcflank.com/test.htm*) detecta qué tan vulnerable es su PC a distintas amenazas desde Internet y si hay algún caballo de Troya activo.
- El servicio 'Security Check' de Symantec (*http://security1.norton.com*) diagnostica las principales vulnerabilidades.
- En WinNuke (*http://www.jtan.com/resources/winnuke.html*) se puede solicitar un ataque de negación de servicios. Si su PC está conectado a una red, la máquina que sufrirá el ataque será el *firewall* o *proxy* de salida a Internet, por lo que este tipo de pruebas deben ser realizadas únicamente en máquinas privadas y a través de conexiones por módem o similares.
- Virtual Suicide (*http://suicide.netfarmers.net*) es una demostración de algunos agujeros de seguridad conocidos. Las pruebas que contiene pueden producir *cuelgues* o pérdida de datos en el equipo que se ejecutan (o en el *proxy*, si estamos conectados a través de una red). El usuario asume la responsabilidad de sus acciones si ejecuta estas demostraciones.

Repita algunas de las pruebas desactivando *Compartir archivos e impresoras* (quizás deberá reinicializar la PC).

Como se mencionó, si Ud. tiene instalado un sistema operativo para servidor (tal como Windows 2000 o Linux) deberá cerrar aquellos puertos que no utilice. Desde Windows 2000 hay que entrar a *Panel de Control* | *Herramientas Administrativas* | *Servicios* y detener todos los servicios innecesarios (por ejemplo, *Servicios simples de TCP/IP,* que engloba al generador de caracteres, hora, desechar, eco y cita del día). En Linux, los servicios telnet, FTP, finger y algunos otros se gestionan desde el archivo */etc/inetd.conf.* También es posible detener demonios temporalmente mediante comandos al estilo de */etc /init.d/inetd stop*.

Las páginas Web pueden contener códigos maliciosos en forma de controles ActiveX, scripts de Visual Basic o applets de Java. En Sandbox Security (*http://www.sandboxsecurity.com*) se encuentran varios análisis para poner a prueba nuestra configuración. Estos tests pueden llegar a bloquear nuestro PC o producir pérdida de datos, por lo que hay que ejecutarlos con precaución. Algunas pruebas consiguen que el sistema se quede sin recursos, agotando toda su memoria o sobrecargando el procesador.

Microsoft ha puesto a disposición una aplicación web denominada Microsoft Personal Security Advisor (MPSA) que permite conocer algunas de las debilidades básicas que puede padecer su sistema Windows NT 4.0 ó Windows 2000. Para realizar la auditoría, acuda a la página: *http://www.microsoft.com/technet/mpsa/start.asp* y pulse el botón *Scan Now*. MPSA escaneará su sistema, generando un informe sobre la configuración de seguridad de su máquina y recomendaciones para su mejora. Puede corregir las deficiencias encontradas y volver a ejecutar el escaneo para comprobar si han desaparecido. Microsoft recomienda ejecutar este escaneo de forma regular para mantenerse al día en materia de seguridad.

Muchas consultoras le cobrarían un ojo de la cara por decirle lo mismo. Así que aproveche la oportunidad.

Fase 6: Elaboración de informe

Después de completar las pruebas y procesar los resultados obtenidos, se debe elaborar un informe final explicando el tipo y el grado de vulnerabilidad encontrado, las consecuencias y la solución recomendada. Todas las bitácoras de las pruebas deben incluirse en un anexo.

Se puede clasificar el grado de vulnerabilidad encontrado con base a la siguiente escala:

- Alto: Corresponde a aquellas vulnerabilidades que comprometen directamente el desempeño y/o funcionamiento del sistema que presta servicio; se cuentan entre éstas las susceptibles a ataques de negación de servicio (DoS), posibilidad de penetración en el sistema para sustraer información o para tener acceso a otros sistemas adyacentes.
- Medio: corresponde a casos en los cuales un atacante es capaz de obtener información de cierta relevancia del sistema debido a que archivos de configuración y logs están disponibles. Esto podría entonces revelar debilidades de tipo alto.
- Bajo: corresponde generalmente a malas configuraciones, por ejemplo en los firewalls, por lo que se puede obtener información acerca de los puertos que están abiertos y que responden a las peticiones de conexión. Dado que los puertos pueden además de estar abiertos a posibles conexiones, ellos pueden estar prestando algún tipo de servicio que no esté protegido y se pasa así a una vulnerabilidad de tipo medio o alto.

ANEXO D

CHECK LIST AUDITORÍA DE BASE DE DATOS

CHECKLIST AUDITORIA DE BASE DE DATOS:

	1. Existe algún archivo de tipo Log donde guarde información referida a las operaciones que realiza la Base de datos?
X	Si
	No
	N/A
	Observaciones:

***REPOSITORIO: SEGURIDAD ***

	2. Se realiza copias de seguridad (diariamente, semanalmente, mensualmente, etc.)?
X	Si
	No
	N/A
	Observaciones:

	3. Existe algún usuario que no sea el DBA pero que tenga asignado el rol DBA del servidor?
X	Si
	No
	N/A
	Observaciones:

	4. Se encuentra un administrador de sistemas en la empresa que lleve un control de los usuario?
	Si
	No
X	N/A
	Observaciones:

	5. Son gestionados los perfiles de estos usuarios por el administrador?
	Si
X	No
	N/A
	Observaciones: el manejo de usuarios se hace a través de la aplicación (sistema para agencia de viajes) y esto se traslada al nivel de la base de datos

	6. Son gestionados los accesos a las instancias de la Base de Datos?
	Si
X	No
	N/A
	Observaciones: la gestión de acceso se hace a nivel de aplicación

7. Las instancias que contienen el repositorio, tienen acceso restringido?	
	Si
	No
	N/A
	Observaciones:

8. Se renuevan las claves de los usuarios de la Base de Datos?	
	Si
X	No
	N/A
	Observaciones:

9. Se obliga el cambio de la contraseña de forma automática?	
	Si
	No
X	N/A
	Observaciones:

10. Se encuentran listados de todos aquellos intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?	
	Si
	No
X	N/A
	Observaciones:

11. Posee la base de datos un diseño físico y lógico?	
	Si
	No
	N/A
	Observaciones:

12. Posee el diccionario de datos un diseño físico y lógico?	
	Si
X	No
	N/A
	Observaciones:

13. Existe una instancia con copia del Repositorio para el entorno de desarrollo?	
X	Si
	No
	N/A
	Observaciones:

14. Está restringido el acceso al entorno de desarrollo?	
	Si
X	No
	N/A
	Observaciones: se trabaja en forma conjunta

15. Los datos utilizados en el entorno de desarrollo, son reales?	
	Si
x	No
	N/A
	Observaciones: algunas veces si, ya que existen tablas con datos específicos que deben se reales para realizar pruebas

16. Se llevan a cabo copias de seguridad del repositorio?	
	Si
	No
	N/A
	Observaciones:

17. Las copias de seguridad se efectúan diariamente?	
	Si
	No
	N/A
	Observaciones:

18. Las copias de seguridad son encriptadas?	
	Si
X	No
	N/A
	Observaciones:

19. Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?	
X	Si
	No
	N/A
	Observaciones:

20. Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?	
	Si
X	No
	N/A
	Observaciones:

21. En caso de que el equipo principal sufra una avería, existen equipos auxiliares?	
	Si
	No
	N/A
	Observaciones:

22. Cuando se necesita restablecer la base de datos, se le comunica al administrador?	
X	Si
	No
	N/A
	Observaciones:

23. La comunicación se establece de forma escrita?	
	Si
X	No
	N/A
	Observaciones:

24. Una vez efectuada la restauración, se le comunica al interesado?	
X	Si
	No
	N/A
	Observaciones:

25. Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?

X	Si
	No
	N/A
	Observaciones: aunque es mínima, después de un tiempo de uso surgen algunas dudas y cuestiones

26. Se documentan los cambios efectuados?	
X	Si
	No
	N/A
	Observaciones: Minimante. Algunos cambios suelen ser no documentados. No hay un seguimiento exhaustivo de los cambios

27. Hay algún procedimiento para dar de alta a un usuario?	
X	Si
	No
	N/A
	Observaciones:

28. Hay algún procedimiento para dar de baja a un usuario?	
X	Si
	No
	N/A
	Observaciones:

29. Es eliminada la cuenta del usuario en dicho procedimiento?	
	Si
X	No
	N/A
	Observaciones: se realiza una eliminación logica

30. El motor de Base de Datos soporta herramientas de auditoria?	
X	Si
	No
	N/A
	Observaciones:

31. Existe algún tipo de documentación referida a la estructura y contenidos de la Base de Datos?

X	Si
	No
	N/A
	Observaciones: documentación extraída de la pagina oficial del motor de base de datos

32. Se cuenta con niveles de seguridad para el acceso a la Base de Datos?	
	Si
X	No
	N/A
	Observaciones:

33. Se encuentra la Base de Datos actualizada con el último Set de Parches de Seguridad?	
	Si
X	No
	N/A
	Observaciones:

34. Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?	
	Si
X	No
	N/A
	Observaciones: solo se restauran los backup realizados

35. Existen logs que permitan tener pistas sobre las acciones realizadas sobre los objetos de las base de datos?	
X	Si
	No
	N/A
	Observaciones:

*** **Si existen estos Logs** ***

36. Se usan los generados por el DBMS?	
X	Si
	No
	N/A
	Observaciones:

	37. Se usan los generados por el Sistema Operativo?
	Si
X	No
	N/A
	Observaciones:

	38. Se han configurado estos logs para que sólo almacenan la información relevante?
	Si
X	No
	N/A
	Observaciones:

	39. Se tiene un sistema de registro de acciones propio, con fines de auditoría?
	Si
	No
X	N/A
	Observaciones:

	40. Las instalaciones del centro de cómputo son resistentes a potenciales daños causados por agua?
	Si
X	No
	N/A
	Observaciones:

	41. Las instalaciones del centro de cómputo son resistentes a potenciales daños causados por el fuego?
	Si
X	No
	N/A
	Observaciones:

	42. La ubicación del centro de cómputo es acorde con las mínimas condiciones de seguridad?
X	Si
	No
	N/A
	Observaciones:

43. Existe y es conocido un plan de actuación para el personal del centro de cómputo, en caso de incidentes naturales u otros que involucren gravemente la instalación?

	Si
	No
X	N/A
	Observaciones:

44. Existe un control de las entradas y las salidas de la base de datos (A nivel datos)?	
X	Si
	No
	N/A
	Observaciones: este tipo de control se usa solo para casos particulares

***Tareas realizadas por terceros ***

45. La información que poseen en la base de datos es real?	
	Si
X	No
	N/A
	Observaciones: algunas veces si, ya que existen tablas con datos específicos que deben se reales para realizar pruebas

46. Existe un contrato de confidencialidad con las terceras partes?	
X	Si
	No
	N/A
	Observaciones:

47. Se notifican las acciones realizadas a nivel de mantenimiento de hardware?	
	Si
X	No
	N/A
	Observaciones:

ANEXO E
GLOSARIO INGLÉS-ESPAÑOL

ISACA® Glossary of Terms
English-Spanish

ACKNOWLEDGMENTS

The 2011 edition of the ISACA® Glossary of Terms has been translated into Spanish (terms only) by a professional translation vendor and reviewed by many volunteers. The verified and approved translation of this glossary will help reduce the time, cost, and inconsistencies of ISACA Spanish translations. All of the ISACA members who participated in the review of the translated glossary deserve our thanks and gratitude.

Expert Translation Reviewers

Sr. Alfonso Javier Mateluna Concha, CISA, CISM, CRISC, Chile
Sr. Arnoldo Altamirano, CISA, Costa Rica
Mr. Daniel Morales, CISA, Costa Rica
Ing. Fabiola Paulina Moyón Constante, CISA, Ecuador
Sr. Juan Davila Ramirez, CISA, CISM, Peru
Sr. Larry Llirán, CISA, CISM, Puerto Rico
Ms. Lolita E. Vargas-DeLeon, CISA, CIA, CPA, MIBA, Puerto Rico
Sr. Luis A. Capua, CISM, CRISC, Argentina
Sr. Luis Diego León, CISA, Costa Rica
Sr. Marco Gámez, CISA, CRISC, Costa Rica
Mrs. Maria Patricia Prandini, CISA, CRISC, Argentina
Lic. Pablo Fernández, CISA, CRISC, Costa Rica
Sr. Salomon Rico, CISA, CISM, CGEIT, Mexico
Sr. Victor Adalmer Vasquez Mejia, CISA, CISM, CRISC, Colombia

FEEDBACK

Later in 2012, we will publish the English-Spanish 2nd edition, which will include updates and revisions. Please contact the ISACA Translation Manager at asalzano@isaca.org for any comments or suggested changes.

ISACA®
Trust in, and value from, information systems

A

Abend An abnormal end to a computer job; termination of a task prior to its completion because of an error condition that cannot be resolved by recovery facilities while the task is executing
SPANISH: **Terminación anormal**

Acceptable interruption window The maximum period of time that a system can be unavailable before compromising the achievement of the organization's business objectives.
SPANISH: **Ventana de interrupción aceptable**

Acceptable use policy A policy that establishes an agreement between users and the organization and defines for all parties' ranges of use that are approved before gaining access to a network or the Internet.
SPANISH: **Política de uso aceptable**

Access control The processes, rules and deployment mechanisms which control access to information systems, resources and physical access to premises
SPANISH: **Control de acceso**

Access control list (ACL) An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals. Scope Note: Access control lists are also referred to as access control tables.
SPANISH: **Lista de control de acceso (ACL)**

Access control table An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals.
SPANISH: **Tabla de control de acceso**

Access method The technique used for selecting records in a file, one at a time, for processing, retrieval or storage. The access method is related to, but distinct from, the file organization, which determines how the records are stored.
SPANISH: **Método de acceso**

Access path The logical route an end user takes to access computerized information. Scope Note: Typically, it includes a route through the operating system, telecommunications software, selected application software and the access control system.
SPANISH: **Ruta de acceso**

Access rights The permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information security policy
SPANISH: **Derechos de acceso**

Access servers Provides centralized access control for managing remote access dial-up services
SPANISH: **Servidores de acceso**

Accountability The ability to map a given activity or event back to the responsible party.
SPANISH: **Responsabilidad**

Accountable party The individual, group, or entity that is ultimately responsible for a subject matter, process or scope. Scope Note: Within ITAF, the term management is equivalent to "accountable party".
SPANISH: **Parte responsable**

Acknowledgement (ACK) A flag set in a packet to indicate to the sender that the previous packet sent was accepted correctly by the receiver without errors, or that the receiver is now ready to accept a transmission.
SPANISH: **Reconocimiento (ACK)**

Active recovery site (Mirrored) Recovery strategy that involves two active sites, each capable of taking over the other's workload in the event of a disaster. Scope Note: Each site will have enough idle processing power to restore data from the other site and to accommodate the excess workload in the event of a disaster.
SPANISH: **Sitio de recuperación activo (espejo)**

Active response A response in which the system either automatically, or in concert with the user, blocks or otherwise affects the progress of a detected attack. Scope Note: The responses takes one of three forms; amending the environment, collecting more information or striking back against the user.
SPANISH: **Respuesta activa**

Activity The main actions taken to operate the COBIT process.
SPANISH: **Actividad**

Address Within computer storage, the code used to designate the location of a specific piece of data
SPANISH: **Dirección**

Address space The number of distinct locations that may be referred to with the machine address Scope Note: For most binary machines, it is equal to 2n, where n is the number of bits in the machine address.
SPANISH: **Espacio de dirección**

Addressing The method used to identify the location of a participant in a network Scope Note: Ideally, addressing specifies where the participant is located rather than who they are (name) or how to get there (routing).
SPANISH: **Direccionamiento**

Adjusting period The calendar can contain "real" accounting periods and/or adjusting accounting periods. The "real" accounting periods must not overlap, and cannot have any gaps between them. Adjusting accounting periods can overlap with other accounting periods. Scope Note: For example, a period called DEC-93 can be defined that includes 01-DEC-1993 through 31-DEC-1993. An adjusting period called DEC31-93 can also be defined that includes only one day: 31-DEC-1993 through 31-DEC-1993.
SPANISH: **Período de ajuste**

Administrative controls The rules, procedures and practices dealing with operational effectiveness, efficiency and adherence to regulations and management policies.
SPANISH: **Controles administrativos**

Adware Any software package that automatically plays, displays or downloads advertising material to a computer after the software is installed on it or while the application is being used Scope Note: In most cases, this is done without any notification to the user or the user's consent. The term adware may also refer to software that displays advertisements, whether or not it does so with the user's consent; such programs display advertisements as an alternative to shareware registration fees. These are classified as "adware" in the sense of advertising-supported software, but not as spyware. Adware in this form does not operate surreptitiously or mislead the user, and provides the user with a specific service.
SPANISH: **Sistemas de publicidad (adware)**

Alert situation The point in an emergency procedure when the elapsed time passes a threshold and the interruption is not resolved. The organization entering into an alert situation initiates a series of escalation steps.
SPANISH: **Situación de alerta**

Allocation entry A recurring journal entry used to allocate revenues or costs. Scope Note: For example, an allocation entry could be defined to allocate costs to each department based on head count.
SPANISH: **Entrada de asignación**

Alpha The use of alphabetic characters or an alphabetic character string
SPANISH: **Alfa**

Alternate facilities Locations and infrastructures from which emergency or backup processes are executed, when the main premises are unavailable or destroyed. Scope Note: This includes other buildings, offices or data processing centers.
SPANISH: **Instalaciones alternas**

Alternate process Automatic or manual processes designed and established to continue critical business processes from point-of-failure to return-to-normal.
SPANISH: **Proceso alterno**

Alternative routing A service that allows the option of having an alternate route to complete a call when the marked destination is not available Scope Note: In signaling, alternate routing is the process of allocating substitute routes for a given signaling traffic stream in case of failure(s) affecting the normal signaling links or routes of that traffic stream.
SPANISH: **Enrutamiento alternativo**

American Standard Code for Information Interchange See ASCII
SPANISH: **Código Estadounidense Estándar para el Intercambio de Información**

Amortization The process of cost allocation that assigns the original cost of an intangible asset to the periods benefited; calculated in the same way as depreciation.
SPANISH: **Amortización**

Analog A transmission signal that varies continuously in amplitude and time and is generated in wave formation Scope Note: Analog signals are used in telecommunications
SPANISH: **Analógico**

Analytical technique The examination of ratios, trends and changes in balances and other values between periods to obtain a broad understanding of the organization's financial or operational position and to identify areas that may require further or closer investigation. Scope Note: This technique is often used when planning the assurance assignment.
SPANISH: **Técnica analítica**

Anomaly Unusual or statistically rare.
SPANISH: **Anomalía**

Anomaly detection Detection on the basis of whether the system activity matched that defined as abnormal.
SPANISH: **Detección de anomalías**

Anonymity The quality or state of not being named or identified.
SPANISH: **Anonimato**

Antivirus software An application software deployed at multiple points in an IT architecture. It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected.
SPANISH: **Software antivirus**

Appearance The act of giving the idea or impression of being or doing something.
SPANISH: **apariencia**

Appearance of independence Behavior adequate to meet the situations occurring during audit work (interviews, meetings, reporting, etc.). Scope Note: The IS auditor should be aware that appearance of independence depends upon the perceptions of others and can be influenced by improper actions or associations.
SPANISH: **Apariencia de independencia**

Applet A program written in a portable, platform independent computer language, such as Java, JavaScript or Visual Basic Scope Note: It is usually embedded in an HTML page downloaded from web servers and then executed by a browser on client machines to run any web-based application (e.g., generate web page input forms, run audio/video programs, etc.). Applets can only perform a restricted set of operations, thus preventing, or at least minimizing, the possible security compromise of the host computers. However, applets expose the user's machine to risks if not properly controlled by the browser, which should not allow an applet to access a machine's information without prior authorization of the user.
SPANISH: **Applet**

Application A computer program or set of programs that perform the processing of records for a specific function Scope Note: An application program contrasts with systems programs, such as an operating system or network control program, and with utility programs, such as copy or sort.
SPANISH: **Aplicación**

Application acquisition review An evaluation of an application system being acquired or evaluated, which considers such matters as: appropriate controls are designed into the system; the application will process information in a complete, accurate and reliable manner; the application will function as intended; the application will function in compliance with any applicable statutory provisions; the system is acquired in compliance with the established system acquisition process.
SPANISH: **Revisión de la adquisición de la aplicación**

Application benchmarking The process of establishing the effective design and operation of automated controls within an application.
SPANISH: **Estudio comparativo de la aplicación**

Application control The policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved
SPANISH: **Control de aplicación**

Application development review An evaluation of an application system under development which considers matters such as: appropriate controls are designed into the system; the application will process information in a complete, accurate and reliable manner; the application will function as intended; the application will function in compliance with any applicable statutory provisions; the system is developed in compliance with the established systems development life cycle process.
SPANISH: **Revisión del desarrollo de la aplicación**

Application implementation review An evaluation of any part of an implementation project. Scope Note: Examples include project management, test plans and user acceptance testing procedures.
SPANISH: **Revisión de la implementación de la aplicación**

Application layer In the Open Systems Interconnection (OSI) communications model, the application layer provides services for an application program to ensure that effective communication with another application program in a network is possible. Scope Note: The application layer is not the application that is doing the communication; it is a service layer that provides these services.
SPANISH: **Capa de aplicación (application layer)**

Application maintenance review An evaluation of any part of a project to perform maintenance on an application system. Scope Note: Examples include project management, test plans and user acceptance testing procedures.
SPANISH: **Revisión del mantenimiento de la aplicación**

Application or managed service provider (ASP/MSP) A third party that delivers and manages applications and computer services, including security services to multiple users via the Internet or a private network.
SPANISH: **Proveedor de servicios administrados o de aplicación (ASP/MSP)**

Application program A program that processes business data through activities such as data entry, update or query Scope Note: It contrasts with systems programs, such as an operating system or network control program, and with utility programs sych as copy or sort.
SPANISH: **Programa de aplicación**

Application programming The act or function of developing and maintaining applications programs in production
SPANISH: **Programación de aplicaciones**

Application programming interface (API) A set of routines, protocols and tools referred to as "building blocks" used in business application software development. Scope Note: A good API makes it easier to develop a program by providing all the building blocks related to functional characteristics of an operating system that applications need to specify, for example, when interfacing with the operating system (e.g., provided by MS-Windows, different versions of UNIX). A programmer would utilize these APIs in developing applications that can operate effectively and efficiently on the platform chosen.
SPANISH: **Interfaz de programación de aplicaciones (API)**

Application proxy A service that connects programs running on internal networks to services on exterior networks by creating two connections, one from the requesting client and another to the destination service.
SPANISH: **Proxy de aplicación**

Application security Refers to the security aspects supported by the application, primarily with regard to the roles or responsibilities and audit trails within the applications.
SPANISH: **Seguridad de la aplicación**

Application service provider (ASP) Also known as managed service provider (MSP), it deploys, hosts and manages access to a packaged application to multiple parties from a centrally managed facility. Scope Note: The applications are delivered over networks on a subscription basis.
SPANISH: **Proveedor de Servicios de aplicación (ASP)**

Application software tracing and mapping Specialized tools that can be used to analyze the flow of data, through the processing logic of the application software, and document the logic, paths, control conditions and processing sequences. Scope Note: Both the command language or job control statements and programming language can be analyzed. This technique includes program/system: mapping, tracing, snapshots, parallel simulations and code comparisons.
SPANISH: **Software de rastreo y mapeo de aplicación**

Application system An integrated set of computer programs designed to serve a particular function that has specific input, processing and output activities. Scope Note: Examples include general ledger, manufacturing resource planning and human resource management.
SPANISH: **Sistema de aplicación**

Architecture Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support the organization's objectives.
SPANISH: **Arquitectura**

Arithmetic logic unit (ALU) The area of the central processing unit that performs mathematical and analytical operations
SPANISH: **Unidad aritmético lógica (ALU)**

Artificial intelligence Advanced computer systems that can simulate human capabilities, such as analysis, based on a predetermined set of rules
SPANISH: **Inteligencia artificial**

ASCII Representing 128 characters, the American Standard Code for Information Interchange (ASCII) code normally uses 7 bits. However, some variations of the ASCII code set allow 8 bits. This 8-bit ASCII code allows 256 characters to be represented.
SPANISH: **ASCII**

Assembler A program that takes as input a program written in assembly language and translates it into machine code or machine language
SPANISH: **Ensamblador**

Assembly language A low-level computer programming language which uses symbolic code and produces machine instructions.
SPANISH: **Lenguaje ensamblador**

Assessment A broad review of the different aspects of a company or function that includes elements not covered by a structured assurance initiative. Scope Note: It might include opportunities for reducing the costs of poor quality, employee perceptions on quality aspects, proposals to senior management on policy, goals, etc.
SPANISH: **Evaluación**

Asset Something of either tangible or intangible value worth protecting including people, information, infrastructure, finances and reputation
SPANISH: **Activos**

Assurance An objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the organization. Scope Note: Examples may include financial, performance, compliance and system security engagements.
SPANISH: **Aseguramiento**

Assurance initiative An objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the organization. Scope Note: Examples may include financial, performance, compliance and system security engagements.
SPANISH: **Iniciativa de aseguramiento**

Asymmetric key (public key) A cipher technique in which different cryptographic keys are used to encrypt and decrypt a message Scope Note: See public key encryption.
SPANISH: **Clave asimétrica (clave pública)**

Asynchronous Transfer Mode (ATM) A high-bandwidth low-delay switching and multiplexing technology that allows integration of real-time voice and video as well as data. It is a data link layer protocol. Scope Note: This means that it is a protocol-independent transport mechanism. ATM allows very high speed data transfer rates at up to 155 Mbit/s.
acronym ATM should not be confused with the alternate usage for ATM which refers to an automated teller machine.
SPANISH: **Modo de Transferencia Asíncrona (ATM)**

Asynchronous transmission Character-at-a-time transmission.
SPANISH: **Transmisión asíncrona**

Attest reporting engagement An engagement where an IS auditor is engaged to either examine management's assertion regarding particular a subject matter or the subject matter directly. Scope Note: The IS auditor's report consists of an opinion on one of the following: The subject matter. These reports relate directly to the subject matter itself rather than an assertion. In certain situations management will not be able to make an assertion over the subject of the engagement. An example of this situation is when IT services are out-sourced to third party. Management will not ordinarily be able to make an assertion over the controls that the third-party is responsible for. Hence, an IS auditor would have to report directly on the subject matter rather than an assertion
SPANISH: **Opinión de un experto independiente**

Attitude Way of thinking, behaving, feeling, etc.
SPANISH: **Actitud**

Attribute sampling An audit technique used to select items from a population for audit testing purposes based on selecting all those items that have certain attributes or characteristics (such as all items over a certain size)
SPANISH: **Muestreo por atributos**

Audit Formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met. Scope Note: An audit may be carried out by internal or external groups.
SPANISH: **Auditoría**

Audit accountability Performance measurement of service delivery including cost, timeliness and quality against agreed service levels.
SPANISH: **Rendición de cuentas de la función de auditoría**

Audit authority A statement of the position within the organization, including lines of reporting and the rights of access.
SPANISH: **Autoridad de auditoría**

Audit charter A document approved by the board, which defines the purpose, authority and responsibility of the internal audit activity.
SPANISH: **Estatuto de la Función de Auditoría**

Audit evidence The information used to support the audit opinion.
SPANISH: **Evidencia de auditoría**

Audit expert systems Expert or decision support systems that can be used to assist IS auditors in the decision-making process by automating the knowledge of experts in the field. Scope Note: This technique includes automated risk analysis, systems software and control objectives software packages.
SPANISH: **Sistemas expertos de auditoría**

Audit objective The specific goal(s) of an audit. Scope Note: These often center on substantiating the existence of internal controls to minimize business risk.
SPANISH: **Objetivo de auditoría**

Audit plan 1. A plan containing the nature, timing and extent of audit procedures to be performed by engagement team members in order to obtain sufficient appropriate audit evidence to form an opinion. Scope Note: The plan includes the areas to be audited, the type of work planned, the high level objectives and scope of the work, and topics such as budget, resource allocation, schedule dates, type of report and its intended audience and other general aspects of the work. 2. A high level description of the audit work to be performed in a certain period of time.
SPANISH: **Plan de auditoría**

Audit program A step-by-step set of audit procedures and instructions that should be performed to complete an audit.
SPANISH: **Programa de auditoría**

Audit responsibility The roles, scope and objectives documented in the service level agreement between management and audit.
SPANISH: **Responsabilidad de la función de Auditoría**

Audit risk The probability that information or financial reports may contain material errors and that the auditor may not detect an error that has occurred.
SPANISH: **Riesgo de auditoría**

Audit sampling The application of audit procedures to less than 100 percent of the items within a population to obtain audit evidence about a particular characteristic of the population.
SPANISH: **Muestreo de auditoría**

Audit trail A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source.
SPANISH: **Pista de auditoría**

Audit universe An inventory of audit areas that is compiled and maintained to identify areas for audit during the audit planning process. Scope Note: Traditionally, the list includes all financial and key operational systems as well as other units that would be audited as part of the overall cycle of planned work. The audit universe serves as the source from which the annual audit schedule is prepared. The universe will be periodically revised to reflect changes in the overall risk profile.
SPANISH: **Universo auditable**

Auditability The level to which transactions can be traced and audited through a system.
SPANISH: **Auditabilidad**

Auditable unit Subjects, units, or systems that are capable of being defined and evaluated. Scope Note: Auditable units may include:
Policies, procedures and practices
Cost centers, profit centers and investment centers
General ledger account balances
Information systems (manual and computerized)
Major contracts and programs
Organizational units, such as product or service lines
Functions, such as information technology, purchasing, marketing, production, finance, accounting and human resources
Transaction systems for activities, such as sales, collection, purchasing, disbursement, inventory and cost accounting, production, treasury, payroll and capital assets
Financial statements
Laws and regulations
SPANISH: **Unidad auditable**

Authentication 1. The act of verifying identity, i.e., user, system Scope Note: Risk: Can also refer to the verification of the correctness of a piece of data 2. The act of verifying the identity of a user, the user's eligibility to access computerized information Scope Note: Assurance: Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data.
SPANISH: **Autenticación**

Automated application controls Controls that have been programmed and embedded within an application.
SPANISH: **Controles automatizados de aplicación**

Availability Information that is accessible when required by the business process now and in the future
SPANISH: **Disponibilidad**

Awareness Being acquainted with, mindful of, conscious of and well informed on a specific subject, which implies knowing and understanding a subject and acting accordingly.
SPANISH: **Concientización**

B

Backbone The main communications channel of a digital network. The part of a network that handles the major traffic. Scope Note: The backbone employs the highest-speed transmission paths in the network and may also run the longest distances. Smaller networks are attached to the backbone, and networks that directly connect to the end user or customer are called "access networks." A backbone can span a geographic area of any size from a single building to an office complex to an entire country. Or, it can be as small as a backplane in a single cabinet.
SPANISH: **Columna vertebral (backbone)**

Backup Files, equipment, data and procedures available for use in the event of a failure or loss, if the originals are destroyed or out of service.
SPANISH: **Respaldo, copia de respaldo/seguridad**

Backup center An alternate facility to continue IT/IS operations when the primary DP center is unavailable.
SPANISH: **Sitio alterno**

Badge A card or other device that is presented or displayed to obtain access to an otherwise restricted facility, as a symbol of authority (ex: police), or as a simple means of identification. Scope Note: Badges are also used in advertising and publicity.
SPANISH: **Placa/Credencial (badge)**

Balanced scorecard (BSC) Developed by Robert S. Kaplan and David P. Norton, a coherent set of performance measures organized into four categories that includes traditional financial measures, but adds customer, internal business process, and learning and growth perspectives
SPANISH: **Cuadro de mando (balanced scorecard)**

Bandwidth The range between the highest and lowest transmittable frequencies. It equates to the transmission capacity of an electronic line and is expressed in bytes per second or Hertz (cycles per second).
SPANISH: **Ancho de banda**

Bar code A printed machine-readable code that consists of parallel bars of varied width and spacing.
SPANISH: **Código de barras**

Base case A standardized body of data created for testing purposes. Scope Note: Users normally establish the data. Base cases validate production application systems and test the ongoing accurate operation of the system.
SPANISH: **Caso base**

Baseband A form of modulation in which data signals are pulsed directly on the transmission medium without frequency division and usually utilize a transceiver. Scope Note: In baseband the entire bandwidth of the transmission medium (e.g., coaxial cable) is utilized for a single channel.
SPANISH: **Banda base**

Batch control Correctness checks built into data processing systems and applied to batches of input data, particularly in the data preparation stage. Scope Note: There are two main forms of batch controls: sequence control, which involves numbering the records in a batch consecutively so that the presence of each record can be confirmed, and control total, which is a total of the values in selected fields within the transactions.
SPANISH: **Control de lotes**

Batch processing The processing of a group of transactions at the same time. Scope Note: Transactions are collected and processed against the master files at a specified time.
SPANISH: **Procesamiento por lotes**

Baud rate The rate of transmission for telecommunication data, expressed in bits per second (bps).
SPANISH: **Velocidad en baudios**

Benchmark A test that has been designed to evaluate the performance of a system. Scope Note: In a benchmark test, a system is subjected to a known workload and the performance of the system against this workload is measured. Typically, the purpose is to compare the measured performance with that of other systems that have been subject to the same benchmark test.
SPANISH: **Análisis comparativo (benchmark)**

Benchmarking A systematic approach to comparing an organization's performance against peers and competitors in an effort to learn the best ways of conducting business. Scope Note: Examples include benchmarking of quality, logistical efficiency and various other metrics.
SPANISH: **Estudio comparativo de mercado**

Benefit In business, an outcome whose nature and value (expressed in various ways) are considered advantageous by an organization.
SPANISH: **Beneficio**

Best practice A proven activity or process that has been successfully used by multiple organizations.
SPANISH: **Mejor práctica**

Binary code A code whose representation is limited to 0 and 1.
SPANISH: **Código binario**

Biometric locks Door and entry locks that are activated by such biometric features as voice, eye retina, fingerprint or signature.
SPANISH: **Bloqueos biométricos**

Biometrics A security technique that verifies an individual's identity by analyzing a unique physical attribute, such as a handprint.
SPANISH: **Biométrica**

Bit-stream image Bit-stream backups, also referred to as mirror image backups, involve the backup of all areas of a computer hard disk drive or other type of storage media. Scope Note: Such backups exactly replicate all sectors on a given storage device including all files and ambient data storage areas.
SPANISH: **Copia de la imagen de un disco duro**

Black box testing A testing approach which focuses on the functionality of the application or product and does not require knowledge of the code intervals.
SPANISH: **Pruebas de caja negra**

Broadband Multiple channels are formed by dividing the transmission medium into discrete frequency segments. Scope Note: Broadband generally requires the use of a modem.
SPANISH: **Banda ancha**

Brouters Devices that perform the functions of both bridges and routers, are called brouters. Scope Note: They operate at both the data link and the network layers. A brouter connects same data link type LAN segments as well as different data link ones, which is a significant advantage. Like a bridge it forwards packets based on the data link layer address to a different network of the same type. Also, whenever required, it processes and forwards messages to a different data link type network based on the network protocol address. When connecting same data link type networks, they are as fast as bridges besides being able to connect different data link type networks.
SPANISH: **Brouters**

Browser A computer program that enables the user to retrieve information that has been made publicly available on the Internet; also, that permits multimedia (graphics) applications on the World Wide Web.
SPANISH: **Explorador (browser)**

Brute force The name given to a class of algorithms that repeatedly try all possible combinations until a solution is found.
SPANISH: **Fuerza bruta**

Brute force attack Repeatedly trying all possible combinations of passwords or encryption keys until the correct one is found.
SPANISH: **Ataque de fuerza bruta**

Budget Estimated cost and revenue amounts for a given range of periods and set of books. Scope Note: There can be multiple budget versions for the same set of books.
SPANISH: **Presupuesto**

Budget formula A mathematical expression used to calculate budget amounts based on actual results, other budget amounts and statistics. Scope Note: With budget formulas, budgets using complex equations, calculations and allocations can be automatically created.
SPANISH: **Fórmula de cálculo de presupuesto**

Budget hierarchy A group of budgets linked together at different levels such that the budgeting authority of a lower-level budget is controlled by an upper-level budget.
SPANISH: **Jerarquía de consolidación de presupuesto**

Budget organization An entity (department, cost center, division or other group) responsible for entering and maintaining budget data.
SPANISH: **Unidad de control y gestión presupuestaria**

Buffer Memory reserved to temporarily hold data to offset differences between the operating speeds of different devices, such as a printer and a computer. Scope Note: In a program, buffers are reserved areas of RAM that hold data while they are being processed.
SPANISH: **Memoria intermedia (buffer)**

Buffer overflow Occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Scope Note: Since buffers are created to contain a finite amount of data, the extra information—which has to go somewhere—can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.
SPANISH: **Desbordamiento del Buffer**

Bulk data transfer A data recovery strategy that includes a recovery from complete backups that are physically shipped off site once a week. Scope Note: Specifically, logs are batched electronically several times daily, and then loaded into a tape library located at the same facility as the planned recovery.
SPANISH: **Transferencia de datos masiva**

Bus Common path or channel between hardware devices. Scope Note: A bus can be between components internal to a computer or between external computers in a communications network.
SPANISH: **Bus**

Bus configuration All devices (nodes) are linked along one communication line where transmissions are received by all attached nodes. Scope Note: This architecture is reliable in very small networks, as well as easy to use and understand. This configuration requires the least amount of cable to connect the computers together and, therefore, is less expensive than other cabling arrangements. It is also easy to extend, and two cables can be easily joined with a connector to make a longer cable for more computers to join the network. A repeater can also be used to extend a bus configuration.
SPANISH: **Configuración del bus**

Business balanced scorecard A tool for managing organizational strategy, which uses weighted measures for the areas of financial performance (lag) indicators, internal operations, customer measurements, learning and growth (lead) indicators combined to rate the organization.
SPANISH: **Cuadros de mando integrales de negocios**

Business case Documentation of the rationale for making a business investment, used both to support a business decision on whether to proceed with the investment and as an operational tool to support management of the investment through its full economic life cycle
SPANISH: **Caso de negocio**

Business continuity plan (BCP) A plan used by an organization to respond to disruption of critical business processes. Depends on the contingency plan for restoration of critical systems
SPANISH: **Plan de continuidad del negocio (BCP)**

Business controls The policies, procedures, practices and organizational structures designed to provide reasonable assurance that the business objectives will be achieved and undesired events will be prevented or detected.
SPANISH: **Controles del negocio**

Business dependency assessment A process of identifying resources critical to the operation of a business process.
SPANISH: **Evaluación de las dependencias del negocio**

Business function An activity an enterprise does, or needs to do, to achieve its objectives.
SPANISH: **Función del Negocio**

Business goal The translation of the enterprise's mission from a statement of intention into performance targets and results
SPANISH: **Objetivo de negocio**

Business impact The net effect, positive or negative, on the achievement of business objectives
SPANISH: **Impacto en el negocio**

Business impact analysis (BIA) A process to determine the impact of losing the support of any resource Scope Note: The business impact analysis assessment study will establish the escalation of that loss overtime. It is predicated on the fact that senior management, when provided reliable data to document the potential impact of a lost resource, can make the appropriate decision.
SPANISH: **Análisis del impacto en el negocio**

Business impact analysis/assessment (BIA)
Evaluating the criticality and sensitivity of information assets
exercise that determines the impact of losing the support of any resource to an organization, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and supporting system Scope Note: This process also includes addressing:
Income loss
Unexpected expense
Legal issues (regulatory compliance or contractual)
Interdependent processes
Loss of public reputation or public confidence
SPANISH: **Análisis de impacto al negocio (BIA)**

Business interruption Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) which disrupts the normal course of business operations at an organization.
SPANISH: **Interrupción del negocio**

Business objective A further development of the business goals into tactical targets and desired results and outcomes
SPANISH: **Objetivo de negocio**

Business process An inter-related set of cross-functional activities or events that result in the delivery of a specific product or service to a customer.
SPANISH: **Proceso de negocio**

Business process integrity Controls over the business processes that are supported by the ERP.
SPANISH: **Integridad del proceso de negocio**

Business process owner The individual responsible for identifying process requirements, approving process design and managing process performance Scope Note: A business process owner must be at an appropriately high level in the enterprise and have authority to commit resources to process-specific risk management activities.
SPANISH: **Dueño del proceso de negocio**

Business process reengineering (BPR) The thorough analysis and significant redesign of business processes and management systems to establish a better performing structure, more responsive to the customer base and market conditions, while yielding material cost savings.
SPANISH: **Reingeniería de los procesos de negocio (BPR).**

Business risk A probable situation with uncertain frequency and magnitude of loss (or gain).
SPANISH: **Riesgo de negocio**

Business service provider (BSP) An ASP that also provides outsourcing of business processes such as payment processing, sales order processing and application development.
SPANISH: **Proveedor de servicios del negocio (BSP)**

Business sponsor The individual accountable for delivering the benefits and value of an IT-enabled business investment program to the organization.
SPANISH: **Patrocinador del negocio**

Business-to-business Transactions where the acquirer is an organization or an individual operating in the ambits of his/her professional activity. In this case, laws and regulations related to consumer protection are not applicable. Scope Note: The contract's general terms should be communicated to the other party and specifically approved. Some companies require the other party to fill out check-boxes where there is a description such as "I specifically approve the clauses…" This is not convincing: the best solution is the adoption of a digital signature scheme, which allows the approval of clauses and terms with the non-repudiation condition.
SPANISH: **De negocio a negocio (Business-to-business)**

Business-to-consumer Selling processes where the involved parties are the organization, which offers goods or services, and a consumer. In this case there is comprehensive legislation which protects the consumer. Scope Note: Comprehensive legislation includes:
Regarding contracts established outside the merchant's property (such as the right to end the contract with full refund or the return policy for goods)
Regarding distance contracts (such as rules which establish how a contract should be written, specific clauses and the need to make it transmitted to the consumer and approved)
Regarding electronic form of the contract (such as on the Internet, the possibility for the consumer to exit from the procedure without having his/her data recorded)
SPANISH: **De negocio a consumidor (Business-to-consumer)**

Business-to-consumer e-commerce (B2C) Refers to the processes by which organizations conduct business electronically with their customers and/or public at large using the Internet as the enabling technology.
SPANISH: **Comercio electrónico de negocio a consumidor (B2C)**

Bypass label processing (BLP) A technique of reading a computer file while bypassing the internal file/data set label. This process could result in bypassing of the security access control system.
SPANISH: **Omisión del procesamiento de etiquetas (bypass label processing, BLP)**

C

Cadbury The Committee on the Financial Aspects of Corporate Governance, set up in May 1991 by the UK Financial Reporting Council, the London Stock Exchange and the UK accountancy profession, was chaired by Sir Adrian Cadbury and produced a report on the subject commonly known, in the UK, as the Cadbury Report.
SPANISH: **Cadbury**

Capability An aptitude, competency or resource that an enterprise may possess or require at an enterprise, business function or individual level that has the potential or is required to contribute to a business outcome and to create value
SPANISH: **Capacidad**

Capability Maturity Model (CMM) 1. Contains the essential elements of effective processes for one or more disciplines
also describes an evolutionary improvement path from ad hoc, immature processes to disciplined, mature processes with improved quality and effectiveness. 2. CMM for software, from the Software Engineering Institute (SEI), is a model used by many organizations to identify best practices useful in helping them assess and increase the maturity of their software development processes Scope Note: CMM ranks software development organizations according to a hierarchy of five process maturity levels. Each level ranks the development environment according to its capability of producing quality software. A set of standards is associated with each of the five levels. The standards for level one describe the most immature or chaotic processes and the standards for level five describe the most mature or quality processes.
maturity model that indicates the degree of reliability or dependency the business can place on a process achieving the desired goals or objectives
collection of instructions an organization can follow to gain better control over its software development process
SPANISH: **Modelo de madurez de capacidad (capability maturity model)**

Capacity stress testing Testing an application with large quantities of data to evaluate its performance during peak periods. It also is called volume testing.
SPANISH: **Prueba de límite de capacidad (capacity stress testing).**

Capital expenditure (CAPEX) An expenditure that is recorded as an asset because it is expected to benefit more than the current period. The asset is then depreciated or amortized over the expected useful life of the asset.
SPANISH: **Gasto de capital (CAPEX)**

Card swipes A physical control technique that uses a secured card or ID to gain access to a highly sensitive location. Scope Note: Card swipes, if built correctly, act as a preventative control over physical access to those sensitive locations. After a card has been swiped, the application attached to the physical card swipe device logs all card users that try to access the secured location. The card swipe device prevents unauthorized access and logs all attempts to enter the secured location.
SPANISH: **Lectura de tarjetas por deslizamiento (card swipes)**

Cathode ray tube (CRT) A vacuum tube that displays data by means of an electron beam striking the screen, which is coated with suitable phosphor material or a device similar to a television screen upon which data can be displayed.
SPANISH: **Tubo de rayos catódicos (CRT)**

Central processing unit (CPU) Computer hardware that houses the electronic circuits that control/direct all operations of the computer system.
SPANISH: **Unidad central de procesamiento (CPU)**

Centralized data processing Identified by one central processor and databases that form a distributed processing configuration.
SPANISH: **Procesamiento centralizado de datos**

Certificate authority (CA) A trusted third party that serves authentication infrastructures or organizations and registers entities and issues them certificates.
SPANISH: **Autoridad del certificado (certificate authority)**

Certificate revocation list (CRL) An instrument for checking the continued validity of the certificates for which the certification authority (CA) has responsibility. Scope Note: CRL details digital certificates that are no longer valid. The time gap between two updates is very critical and is also a risk in digital certificates verification.
SPANISH: **Lista de revocación de certificados (CRL)**

Certification practice statement (CPS) A detailed set of rules governing the certificate authority's operations. It provides an understanding of the value and trustworthiness of certificates issued by a given CA. Scope Note: In terms of the controls that an organization observes, the method it uses to validate the authenticity of certificate applicants and the CA's expectations of how its certificates may be used.
SPANISH: **Declaración de prácticas de certificación (CPS)**

Chain of custody A legal principle regarding the validity and integrity of evidence. It requires accountability for anything that will be used as evidence in a legal proceeding, to ensure that it can be accounted for from the time it was collected until the time it is presented in a court of law. Scope Note: Includes documentation as to who had access to the evidence and when, as well as the ability to identify evidence as being the exact item that was recovered or tested. Lack of control over evidence can lead to it being discredited. Chain of custody depends on the ability to verify that evidence could not have been tampered with. This is accomplished by sealing off the evidence, so it cannot be changed, and providing a documentary record of custody to prove that the evidence was at all times under strict control and not subject to tampering.
SPANISH: **Cadena de custodia**

Challenge/response token A method of user authentication that is carried out through use of the Challenge Handshake Authentication Protocol (CHAP). Scope Note: When a user tries to log into the server using CHAP, the server sends the user a "challenge," which is a random value. The user enters a password, which is used as an encryption key to encrypt the "challenge" and return it to the server. The server is aware of the password. It, therefore, encrypts the "challenge" value and compares it with the value received from the user. If the values match, the user is authenticated. The challenge/response activity continues throughout the session and this protects the session from password sniffing attacks. In addition, CHAP is not vulnerable to "man in the middle" attacks as the challenge value is a random value that changes on each access attempt.
SPANISH: **Token de desafío/respuesta (challenge/response token)**

Change management A holistic and proactive approach to managing the transition from a current to a desired organizational state, focusing specifically on the critical human or "soft" elements of change. Scope Note: Change management includes activities such as culture change (values, beliefs and attitudes), development of reward systems (measures and appropriate incentives), organizational design, stakeholder management, human resource policies and procedures, executive coaching, change leadership training, team building and communications planning and execution.
SPANISH: **Gestión de cambios**

Channel service unit/dgital service unit (CSU/DSU) Interfaces at the physical layer of the OSI reference model, data terminal equipment (DTE) to data circuit terminating equipment (DCE), for switched carrier networks
SPANISH: **Unidad de servicio de canal/unidad de servicio digital (CSU/DSU)**

Chargeback The redistribution of expenditures to the units within a company that gave rise to them. Scope Note: Chargeback is important because without such a policy, misleading views may be given as to the real profitability of a product or service, as certain key expenditures will be ignored or calculated according to an arbitrary formula.
SPANISH: **Prorrateo de costos**

Check digit A numeric value, which has been calculated mathematically, is added to data to ensure that original data have not been altered or that an incorrect, but valid match has occurred. Scope Note: Check digit control is effective in detecting transposition and transcription errors.
SPANISH: **dígito de control (check digit)**

Check digit verification (self-checking digit) A programmed edit or routine that detects transposition and transcription errors by calculating and checking the check digit.
SPANISH: **Verificación del dígito de control (check digit)**

Checklist A list of items that is used to verify the completeness of a task or goal. Scope Note: A checklist is used in quality assurance (and in general, in information systems audit), to check process compliance, code standardization and error prevention, and other items for which consistency processes or standards have been defined.
SPANISH: **Lista de comprobación (checklist)**

Checkpoint restart procedures A point in a routine at which sufficient information can be stored to permit restarting the computation from that point.
SPANISH: **Procedimientos de reinicio desde el punto de verificación (checkpoint restart procedures)**

Checksum A mathematical value that is assigned to a file and used to "test" the file at a later date to verify that the data contained in the file has not been maliciously changed. Scope Note: A cryptographic checksum is created by performing a complicated series of mathematical operations (known as a cryptographic algorithm) that translates the data in the file into a fixed string of digits called a hash value, which is then used as the checksum. Without knowing which cryptographic algorithm was used to create the hash value, it is highly unlikely that an unauthorized person would be able to change data without inadvertently changing the corresponding checksum. Cryptographic checksums are used in data transmission and data storage. Cryptographic checksums are also known as message authentication codes, integrity check-values, modification detection codes or message integrity codes.
SPANISH: **Suma de comprobación (checksum)**

Chief executive officer (CEO) Chief executive officer is the highest ranking individual in an organization.
SPANISH: **Director general ejecutivo (CEO)**

Chief financial officer (CFO) Chief financial officer is the individual primarily responsible for managing the financial risks of an organization.
SPANISH: **Director general financiero (CFO)**

Chief information officer (CIO) The most senior official of the enterprise who is accountable for IT advocacy, aligning IT and business strategies, and planning, resourcing and managing the delivery of IT services, information and the deployment of associated human resources. Scope Note: In some cases, the CIO role has been expanded to become the chief knowledge officer, CKO, who deals in knowledge, not just information. Also see chief technology officer.
SPANISH: **Director de Informática (CIO)**

Chief technology officer (CTO) The individual who focuses on technical issues in an organization. Scope Note: The title CTO is often viewed as synonymous with chief information officer.
SPANISH: **Director general de tecnología (CTO)**

Ciphertext Information generated by an encryption algorithm to protect the plaintext and is unintelligible to the unauthorized reader.
SPANISH: **Texto codificado**

Circuit-switched network A data transmission service requiring the establishment of a circuit-switched connection before data can be transferred from source data terminal equipment (DTE) to a sink DTE. Scope Note: A circuit-switched data transmission service uses a connection network.
SPANISH: **Red de circuito conmutado (circuit-switched network)**

Circular routing In open systems architecture, circular routing is the logical path of a message in a communications network based on a series of gates at the physical network layer in the open systems interconnection (OSI) model.
SPANISH: **Enrutamiento circular**

Cleartext Data that is not encrypted. Also known as plaintext.
SPANISH: **Texto claro**

Client-server A group of computers connected by a communications network, where the client is the requesting machine and the server is the supplying machine. Scope Note: Software is specialized at both ends. Processing may take place on either the client or the server but it is transparent to the user.
SPANISH: **Cliente-servidor**

Cluster controller A communications terminal control hardware unit that controls a number of computer terminals. Scope Note: All messages are buffered by the controller and then transmitted to the receiver.
SPANISH: **Controlador de procesadores múltiples (cluster controller)**

Coaxial cable Composed of an insulated wire that runs through the middle of each cable, a second wire that surrounds the insulation of the inner wire like a sheath, and the outer insulation which wraps the second wire. Scope Note: Coaxial cable has a greater transmission capacity than standard twisted-pair cables but has a limited range of effective distance.
SPANISH: **Cable coaxial**

COBIT Control Objectives for Information and related Technology (COBIT) is a complete, internationally accepted process framework for IT that supports business and IT executives and management in their definition and achievement of business goals and related IT goals by providing a comprehensive IT governance, management, control and assurance model. 'COBIT describes IT processes and associated control objectives, management guidelines (activities, accountabilities, responsibilities and performance metrics) and maturity models. COBIT supports enterprise management in the development, implementation, continuous improvement and monitoring of good IT-related practices. Scope Note: Adoption and use of the COBIT framework are supported by guidance for executives and management (Board Briefing on IT Governance, 2nd Edition), IT governance implementers (COBIT Quickstart, 2nd Edition; IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition; and COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance), and IT assurance and audit professionals (IT Assurance Guide Using COBIT). Guidance also exists to support its applicability for certain legislative and regulatory requirements (e.g., IT Control Objectives for Sarbanes-Oxley, IT Control Objectives for Basel II) and its relevance to information security (COBIT Security Baseline). COBIT is mapped to other frameworks and standards to illustrate complete coverage of the IT management life cycle and support its use in enterprises using multiple IT-related framework and standards.
SPANISH: **COBIT**

COCO Criteria of Control, published by the Canadian Institute of Chartered Accountants in 1995.
SPANISH: **COCO**

Coevolving Originated as a biological term, refers to the way two or more ecologically interdependent species become intertwined over time. Scope Note: As these species adapt to their environment, they also adapt to one another. Today's multi-business companies need to take their cue from biology to survive: They should assume that links among businesses are temporary and that the number of connections—not just their content—matters. Rather than plan collaborative strategy from the top, as traditional companies do, corporate executives in coevolving companies should simply set the context and let collaboration (and competition) emerge from business units.
SPANISH: **Co-evolución**

Coherence Establishing a potent binding force and sense of direction and purpose for the organization, relating different parts of the organization to each other and to the whole to act as a seemingly unique entity.
SPANISH: **Coherencia**

Cohesion The extent to which a system unit--subroutine, program, module, component, subsystem--performs a single dedicated function. Scope Note: Generally, the more cohesive are units, the easier it is to maintain and enhance a system, since it is easier to determine where and how to apply a change.
SPANISH: **Cohesión**

Cold site An IS backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. Scope Note: The site is ready to receive the necessary replacement computer equipment in the event the users have to move from their main computing location to the alternative computer facility.
SPANISH: **Cold site**

Combined Code on Corporate Governance The consolidation in 1998 of the "Cadbury," "Greenbury" and "Hampel" Reports. Scope Note: Named after the Committee Chairs, these reports were sponsored by the UK Financial Reporting Council, the London Stock Exchange, the Confederation of British Industry, the Institute of Directors, the Consultative Committee of Accountancy Bodies, the National Association of Pension Funds and the Association of British Insurers to address the Financial Aspects of Corporate Governance, Directors' Remuneration and the implementation of the Cadbury and Greenbury recommendations.
SPANISH: **Código combinado sobre el gobierno corporativo**

Communication processor A computer embedded in a communications system that generally performs basic tasks of classifying network traffic and enforcing network policy functions. Scope Note: An example is the message data processor of a DDN switching center. More advanced communications processors may perform additional functions.
SPANISH: **Procesador de comunicaciones**

Communications controller Small computers used to connect and coordinate communication links between distributed or remote devices and the main computer, thus freeing the main computer from this overhead function.
SPANISH: **Controlador de comunicaciones**

Community strings Authenticate access to management information base (MIB) objects and function as embedded passwords. Scope Note: Examples are:
Read-only (RO)—Gives read access to all objects in the MIB except the community strings, but does not allow write access
Read-write (RW)—Gives read and write access to all objects in the MIB, but does not allow access to the community strings
Read-write-all—Gives read and write access to all objects in the MIB, including the community strings (only valid for Catalyst 4000, 5000 and 6000 series switches)
community strings are sent across the network in cleartext. The best way to protect an OS software-based device from unauthorized SNMP management is to build a standard IP access list that includes the source address of the management station(s). Multiple access lists can be defined and tied to different community strings. If logging is enabled on the access list, then log messages are generated every time the device is accessed from the management station. The log message records the source IP address of the packet.
SPANISH: **Community strings**

Comparison program A program for the examination of data, using logical or conditional tests to determine or to identify similarities or differences.
SPANISH: **Programa de comparación**

Compensating control An internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions.
SPANISH: **Control compensatorio**

Competencies The strengths of an organization, what it does well. Scope Note: Competencies can refer to the knowledge, skills and abilities of the assurance team or individuals conducting the work.
SPANISH: **Competencias**

Compiler A program that translates programming language (source code) into machine executable instructions (object code).
SPANISH: **Compilador**

Completely connected (mesh) configuration A network topology in which devices are connected with many redundant interconnections between network nodes (primarily used for backbone networks).
SPANISH: **Configuración (malla) conectada por completo**

Completeness check A procedure designed to ensure that no fields are missing from a record.
SPANISH: **Prueba de completitud**

Compliance testing Tests of control designed to obtain audit evidence on both the effectiveness of the controls and their operation during the audit period.
SPANISH: **Pruebas de cumplimiento**

Component A general term that is used to mean one part of something more complex. Scope Note: For example, a computer system may be a component of an IT service, or an application may be a component of a release unit. Components are co-operating packages of executable software that make their services available through defined interfaces. Components used in developing systems may be commercial off-the-shelf software (COTS) or may be purposely built. However, the goal of component-based development is to ultimately use as much pre-developed, prelisted components as possible.
SPANISH: **Componente**

Comprehensive audit An audit designed to determine the accuracy of financial records, as well as evaluate the internal controls of a function or department.
SPANISH: **Auditoría Integral**

Computationally greedy Requiring a great deal of computing power; processor intensive.
SPANISH: **Intensivamente demandante de recursos de procesamiento**

Computer emergency response team (CERT) A group of people integrated at the organization with clear lines of reporting and responsibilities for standby support in case of an information systems emergency group will act as an efficient corrective control, and should also act as a single point of contact for all incidents and issues related to information systems.
SPANISH: **Equipo de respuesta a emergencias de cómputo (CERT)**

Computer forensics The application of the scientific method to digital media to establish factual information for judicial review. Scope Note: This process often involves investigating computer systems to determine whether they are or have been used for illegal or unauthorized activities. As a discipline, it combines elements of law and computer science to collect and analyze data from information systems (e.g., personal computers, networks, wireless communications and digital storage devices) in a way that is admissible as evidence in a court of law.
SPANISH: **Informática forense**

Computer sequence checking Verifies that the control number follows sequentially and any control numbers out of sequence are rejected or noted on an exception report for further research.
SPANISH: **Verificación de la secuencia informática**

Computer server 1. A computer dedicated to servicing requests for resources from other computers on a network. Servers typically run network operating systems. 2. A computer that provides services to another computer (the client).
SPANISH: **Servidor**

Computer-aided software engineering (CASE) The use of software packages that aid in the development of all phases of an information system. Scope Note: System analysis, design programming and documentation are provided. Changes introduced in one CASE chart will update all other related charts automatically. CASE can be installed on a microcomputer for easy access.
SPANISH: **Ingeniería de software asistida por computador (CASE)**

Computer-assisted audit technique (CAAT) Any automated audit technique, such as generalized audit software, test data generators, computerized audit programs and specialized audit utilities.
SPANISH: **Técnica de auditoría asistida por computador (CAAT)**

Concurrency control Refers to a class of controls used in database management systems (DBMS) to ensure that transactions are processed in an atomic, consistent, isolated and durable manner (ACID). This implies that only serial and recoverable schedules are permitted, and that committed transactions are not discarded when undoing aborted transactions.
SPANISH: **Control de concurrencia**

Concurrent access A fail-over process, in which all nodes run the same resource group (there can be no IP or MAC addresses in a concurrent resource group) and access the external storage concurrently.
SPANISH: **Acceso simultáneo**

Confidentiality The protection of sensitive or private information from unauthorized disclosure.
SPANISH: **Confidencialidad**

Configurable controls Typically, automated controls that are based on and, therefore, dependent on the configuration of parameters within the application system.
SPANISH: **Controles configurables**

Configuration item (CI) Component of an infrastructure--or an item, such as a request for change, associated with an infrastructure--which is (or is to be) under the control of configuration management. Scope Note: CIs may vary widely in complexity, size and type, from an entire system (including all hardware, software and documentation) to a single module or a minor hardware component.
SPANISH: **Elemento de configuración (CI)**

Configuration management The control of changes to a set of configuration items over a system life cycle.
SPANISH: **Gestión de la configuración**

Console log An automated detail report of computer system activity.
SPANISH: **Registro (log) de consola**

Consulted In a RACI chart, refers to those people whose opinions are sought on an activity (two-way communication).
SPANISH: **Consultada**

Content filtering Controlling access to a network by analyzing the contents of the incoming and outgoing packets and either letting them pass or denying them based on a list of rules. Scope Note: Content filtering differs from packet filtering in that it is the data in the packet that are analyzed instead of the attributes of the packet itself (e.g., source/target IP address, TCP flags).
SPANISH: **Filtrado de contenido**

Context Includes the factors that must be present before any specific attempt to transform enterprise systems data into knowledge and results. Scope Note: Context includes technology context (technological factors that affect an organization's ability to extract value from data), data context (data accuracy, availability, currency and quality), skills and knowledge (general experience and analytical, technical and business skills), organizational and cultural context (political factors and whether the organization prefers data to intuition) and strategic context (strategic objectives of the organization).
SPANISH: **Contexto**

Contingency plan A plan used by an organization or business unit to respond to a specific systems failure or disruption.
SPANISH: **Plan de contingencias**

Contingency planning Process of developing advance arrangements and procedures that enable an organization to respond to an event that could occur by chance or unforeseen circumstances.
SPANISH: **Planificación de contingencia**

Continuity Preventing, mitigating and recovering from disruption. Scope Note: The terms "business resumption planning"," disaster recovery planning" and "contingency planning" also may be used in this context; they all concentrate on the recovery aspects of continuity.
SPANISH: **Continuidad**

Continuous auditing approach This approach allows IS auditors to monitor system reliability on a continuous basis and to gather selective audit evidence through the computer.
SPANISH: **Enfoque de auditoría continua**

Continuous availability Nonstop service, with no lapse in service; the highest level of service in which no downtime is allowed.
SPANISH: **Disponibilidad continua**

Continuous improvement The goals of continuous improvement (Kaizen) include the elimination of waste, defined as "activities that add cost but do not add value;" just-in-time delivery; production load leveling of amounts and types; standardized work; paced moving lines; right-sized equipment. Scope Note: A closer definition of the Japanese usage of Kaizen is "to take it apart and put back together in a better way." What is taken apart is usually a process, system, product or service. Kaizen is a daily activity whose purpose goes beyond improvement. It is also a process that, when done correctly, humanizes the workplace, eliminates hard work (both mental and physical), and teaches people how to do rapid experiments using the scientific method and how to learn to see and eliminate waste in business processes.
SPANISH: **Mejora continua**

Control center Hosts the recovery meetings where disaster recovery operations are managed.
SPANISH: **Centro de control**

Control framework A set of fundamental controls that facilitates the discharge of business process owner responsibilities to prevent financial or information loss in an organization
SPANISH: **Marco conceptual de control**

Control group Members of the operations area that are responsible for the collection, logging and submission of input for the various user groups.
SPANISH: **Grupo de control**

Control objective A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process.
SPANISH: **Objetivo de control**

Control Objectives for Enterprise Governance A discussion document which sets out an "enterprise governance model" focusing strongly on both the enterprise business goals and the information technology enablers, which facilitate good enterprise governance, published by the Information Systems Audit and Control Foundation in 1999.
SPANISH: **Objetivos de control para el gobierno de la empresa**

Control perimeter The boundary defining the scope of control authority for an entity. Scope Note: For example, if a system is within the control perimeter, the right and ability exists to control it in response to an attack.
SPANISH: **Perímetro de control**

Control practice Key control mechanism that supports the achievement of control objectives through responsible use of resources, appropriate management of risk and alignment of IT with business.
SPANISH: **Práctica de control**

Control risk The risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal controls. (See also inherent risk)
SPANISH: **Riesgo de control**

Control risk self-assessment A method/process by which management and staff of all levels collectively identify and evaluate risks and controls with their business areas. This may be under the guidance of a facilitator such as an auditor or risk manager.
SPANISH: **Autovaloración de riesgos de control**

Control section The area of the central processing unit (CPU) that executes software, allocates internal memory and transfers operations between the arithmetic-logic, internal storage and output sections of the computer.
SPANISH: **Sección de control**

Control weakness A deficiency in the design or operation of a control procedure. Control weaknesses can potentially result in risks relevant to the area of activity not being reduced to an acceptable level (relevant risks are those that threaten achievement of the objectives relevant to the area of activity being examined). Control weaknesses can be material when the design or operation of one or more control procedures does not reduce to a relatively low level the risk that misstatements caused by illegal acts or irregularities may occur and not be detected by the related control procedures.
SPANISH: **Debilidad de controles**

Controls Scope Note: See internal control.
SPANISH: **Controles**

Cookie A message kept in the web browser for the purpose of identifying users and possibly preparing customized web pages for them. Scope Note: For the first time a cookie is set, a user may be required to go through a registration process. Subsequent to this, whenever the cookie's message is sent to the server, a customized view, based on that user's preferences, can be produced. The browser's implementation of cookies has however brought several security concerns, allowing breaches of security and the theft of personal information (e.g., user passwords that validate the user's identity and enable restricted web services).
SPANISH: **Cookie**

Corporate exchange rate An exchange rate, which can be used optionally to perform foreign currency conversion. The corporate exchange rate is generally a standard market rate determined by senior financial management for use throughout the organization.
SPANISH: **Tipo de cambio de la organización**

Corporate governance The system by which organizations are directed and controlled. Boards of directors are responsible for the governance of their organizations. It consists of the leadership and organizational structures and processes that ensure the organization sustains and extends strategies and objectives.
SPANISH: **Gobierno corporativo (corporate governance)**

Corporate security officer (CSO) Responsible for coordinating the planning, development, implementation, maintenance and monitoring of the information security program.
SPANISH: **Director de seguridad corporativa (CSO)**

Corrective controls Designed to correct errors, omissions and unauthorized uses and intrusions, once they are detected.
SPANISH: **Controles correctivos**

COSO Committee of Sponsoring Organizations of the Treadway Commission. Scope Note: Its 1992 report "Internal Control--Integrated Framework" is an internationally accepted standard for corporate governance. See www.coso.org.
SPANISH: **COSO**

Countermeasure Any process that directly reduces a threat or vulnerability.
SPANISH: **Contramedida**

Coupling Measure of interconnectivity among software program modules' structure. Coupling depends on the interface complexity between modules. This can be defined as the point at which entry or reference is made to a module, and what data passes across the interface. Scope Note: In application software design, it is preferable to strive for the lowest possible coupling between modules. Simple connectivity among modules results in software that is easier to understand and maintain and is less prone to a ripple or domino effect caused when errors occur at one location and propagate through the system.
SPANISH: **Modularidad de las interfaces**

Coverage The proportion of known attacks detected by an intrusion detection system.
SPANISH: **Cobertura**

Crack To "break into" or "get around" a software program. Scope Note: For example, there are certain newsgroups that post serial numbers for pirated versions of software. A cracker may download this information in an attempt to crack the program so he/she can use it. It is commonly used in the case of cracking (unencrypting) a password or other sensitive data.
SPANISH: **Crack**

Credentialed analysis In vulnerability analysis, passive monitoring approaches in which passwords or other access credentials are required. Scope Note: Credentialed analysis usually involves accessing a system data object.
SPANISH: **Análisis de credenciales**

Criteria The standards and benchmarks used to measure and present the subject matter and against which the IS auditor evaluates the subject matter. Scope Note: Criteria should be: Objective - Free from bias; Measurable - Provide for consistent measurement; Complete - Include all relevant factors to reach a conclusion; Relevant - Relate to the subject matter. an attestation engagement, benchmarks against which management's written assertion on the subject matter can be evaluated. The practitioner forms a conclusion concerning subject matter by referring to suitable criteria.
SPANISH: **Criterio**

Critical functions Business activities or information that could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization.
SPANISH: **Funciones críticas**

Critical infrastructure Systems whose incapacity or destruction would have a debilitating effect on the economic security of an organization, community or nation.
SPANISH: **Infraestructura crítica**

Critical success factors (CSFs) The most important issues or actions for management to achieve control over and within its IT processes.
SPANISH: **Factores críticos para el éxito (CSF)**

Criticality analysis An analysis to evaluate resources or business functions to identify their importance to the organization, and the impact if a function cannot be completed or a resource is not available.
SPANISH: **Análisis de criticidad**

Cross-certification A certificate issued by one certification authority to a second certification authority so that users of the first certification authority are able to obtain the public key of the second certification authority and verify the certificates it has created. Scope Note: Often cross certification refers specifically to certificates issued to each other by two CAs at the same level in a hierarchy.
SPANISH: **Certificación cruzada**

Cryptography The art of designing, analyzing and attacking cryptographic schemes.
SPANISH: **Criptografía**

Customer relationship management (CRM) A way to identify, acquire and retain customers. CRM is also an industry term for software solutions that help an organization manage customer relationships in an organized manner.
SPANISH: **Gestión de relaciones con clientes (CRM)**

Cybercops An investigator of computer-crime-related activities.
SPANISH: **Cybercops**

D

Damage evaluation The determination of the extent of damage that is necessary to provide for an estimation of the recovery time frame and the potential loss to the organization.
SPANISH: **Evaluación del daño**

Dashboard A tool for setting expectations for an organization at each level of responsibility and continuous monitoring of the performance against set targets.
SPANISH: **Dashboard**

Data analysis Typically in large organizations, where the quantum of data processed by the ERPs are extremely voluminous, analysis of patterns and trends proves to be extremely useful in ascertaining the efficiency and effectiveness of operations. Scope Note: Most ERPs provide opportunities for extraction and analysis of data, some with built-in tools, through the use of third-party developed tools that interface with the ERP systems
SPANISH: **Análisis de datos**

Data classification The assignment of a level of sensitivity to data (or information) that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as data are created, amended, enhanced, stored or transmitted. The classification level is an indication of the value or importance of the data to the organization.
SPANISH: **Clasificación de datos**

Data classification scheme An enterprise scheme for classifying data by factors such as criticality, sensitivity and ownership.
SPANISH: **Esquema de clasificación de datos**

Data communications The transfer of data between separate computer processing sites/devices using telephone lines, microwave and/or satellite links.
SPANISH: **Comunicación de datos**

Data custodian The individuals and departments responsible for the storage and safeguarding of computerized data
SPANISH: **Custodio de datos (data custodian)**

Data dictionary A database that contains the name, type, range of values, source and authorization for access for each data element in a database. It also indicates which application programs use that data so that when a data structure is contemplated, a list of the affected programs can be generated. Scope Note: The data dictionary may be a stand-alone information system used for management or documentation purposes, or it may control the operation of a database.
SPANISH: **Diccionario de datos**

Data diddling Changing data with malicious intent before or during input into the system.
SPANISH: **Cambio malintencionado de datos (diddling)**

Data Encryption Standard (DES) An algorithm for encoding binary data. Scope Note: It is a private key cryptosystem published by the National Bureau of Standards (NBS), the predecessor of the US National Institute of Standards and Technology (NIST). DES was defined as a Federal Information Processing Standard (FIPS) in 1976 and has been used commonly for data encryption in the forms of software and hardware implementation.
SPANISH: **Estándar de encriptación de datos (DES)**

Data flow The flow of data from the input (in Internet banking, ordinarily user input at his/her desktop) to output (in Internet banking, ordinarily data in a bank's central database). Data flow includes traveling through the communication lines, routers, switches and firewalls as well as processing through various applications on servers which process the data from user fingers to storage in a bank's central database.
SPANISH: **Flujo de datos**

Data integrity The property that data meet with a priority expectation of quality and that the data can be relied upon.
SPANISH: **Integridad de datos**

Data leakage Siphoning out or leaking information by dumping computer files or stealing computer reports and tapes.
SPANISH: **Fuga de datos**

Data normalization A structured process for organizing data into tables in such a way that it preserves the relationships among the data.
SPANISH: **Normalización de datos**

Data owner The individuals, normally managers or directors, who have responsibility for the integrity, accurate reporting and use of computerized data
SPANISH: **Propietario de los datos**

Data security Those controls that seek to maintain confidentiality, integrity and availability of information.
SPANISH: **Seguridad de los datos**

Data structure The relationships among files in a database and among data items within each file.
SPANISH: **Estructura de datos**

Data warehouse A generic term for a system that stores, retrieves and manages large volumes of data. Scope Note: Data warehouse software often includes sophisticated comparison and hashing techniques for fast searches, as well as advanced filtering.
SPANISH: **Almacén de datos (Data warehouse)**

Database A stored collection of related data needed by organizations and individuals to meet their information processing and retrieval requirements.
SPANISH: **Base de datos**

Database administrator (DBA) An individual or department responsible for the security and information classification of the shared data stored on a database system. This responsibility includes the design, definition and maintenance of the database.
SPANISH: **Administrador de base de datos (DBA)**

Database management system (DBMS) A software system that controls the organization, storage and retrieval of data in a database.
SPANISH: **Sistemas de gestión de base de datos (DBMS)**

Database replication The process of creating and managing duplicate versions of a database. Scope Note: Replication not only copies a database but also synchronizes a set of replicas so that changes made to one replica are reflected in all the others. The beauty of replication is that it enables many users to work with their own local copy of a database but have the database updated as if they were working on a single centralized database. For database applications where geographically users are distributed widely, replication is often the most efficient method of database access.
SPANISH: **Replicación de la base de datos**

Database specifications These are the requirements for establishing a database application. They include field definitions, field requirements and reporting requirements for the individual information in the database.
SPANISH: **Especificaciones de base de datos**

Datagram A packet (encapsulated with a frame containing information), which is transmitted in a packet-switching network from source to destination.
SPANISH: **Datagrama**

Data-oriented systems development Focuses on providing ad hoc reporting for users by developing a suitable accessible database of information and to provide useable data rather than a function.
SPANISH: **Desarrollo de sistemas orientado a datos**

Decentralization The process of distributing computer processing to different locations within an organization.
SPANISH: **Descentralización**

Decision support systems (DSS) An interactive system that provides the user with easy access to decision models and data, to support semi structured decision-making tasks.
SPANISH: **Sistemas de apoyo a la decisión (DSS)**

Decryption A technique used to recover the original plaintext from the ciphertext such that it is intelligible to the reader. The decryption is a reverse process of the encryption.
SPANISH: **Desencriptación, descifrado**

Decryption key A digital piece of information used to recover plaintext from the corresponding ciphertext by decryption.
SPANISH: **Llave/Clave de desencriptación/descifrado**

Default A computer software setting or preference that states what will automatically happen in the event that the user has not stated another preference. For example, a computer may have a default setting to launch or start Netscape whenever a GIF file is opened; however, if using Photoshop is the preference for viewing a GIF file, the default setting can be changed to Photoshop. In the case of default accounts, these are accounts that are provided by the operating system vendor (e.g., root in UNIX).
SPANISH: **Valores predeterminados**

Default deny policy A policy whereby access is denied unless it is specifically allowed. The inverse of default allow.
SPANISH: **Política de negación predeterminada**

Default password The password used to gain access when a system is first installed on a computer or network device. Scope Note: There is a large list published on the Internet and maintained at several locations. Failure to change these after the installation leaves the system vulnerable.
SPANISH: **Contraseña predeterminada**

Defense in depth The practice of layering defenses to provide added protection. Defense in depth increases security by raising the effort needed in an attack. This strategy places multiple barriers between an attacker and an organization's computing and information resources.
SPANISH: **Defensa en profundidad**

Degauss The application of variable levels of alternating current for the purpose of demagnetizing magnetic recording media. Scope Note: The process involves increasing the alternating current field gradually from zero to some maximum value and back to zero, leaving a very low residue of magnetic induction on the media. Degauss loosely means to erase.
SPANISH: **Desmagnetizar (degauss)**

Demodulation The process of converting an analog telecommunications signal into a digital computer signal.
SPANISH: **Demodulación**

Demographic A fact determined by measuring and analyzing data about a population; it relies heavily upon survey research and census data.
SPANISH: **Demográfico**

Denial-of-service attack (DoS) An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate.
SPANISH: **Ataque de denegación de servicio**

Depreciation The process of cost allocation that assigns the original cost of equipment to the periods benefited. Scope Note: The most common method of calculating depreciation is the straight-line method, which assumes that assets should be written off in equal amounts over their lives.
SPANISH: **Depreciación**

Detailed IS controls Controls over the acquisition, implementation, delivery and support of IS systems and services made up of application controls plus those general controls not included in pervasive controls.
SPANISH: **Controles detallados de SI**

Detective application controls Controls designed to detect errors that may have occurred, based on predefined logic or business rules. Detective application controls are usually executed after an action has taken place and often cover a group of transactions.
SPANISH: **Controles detectivos de aplicación**

Detective controls Controls that exist to detect and report when errors, omissions and unauthorized uses or entries occur
SPANISH: **Controles detectivos**

Device A generic term for a computer subsystem, such as a printer, serial port, or disk drive. A device frequently requires its own controlling software, called a device driver.
SPANISH: **Dispositivo**

Dial-back Used as a control over dial-up telecommunications lines. The telecommunications link established through dial-up into the computer from a remote location is interrupted so the computer can dial back to the caller. The link is permitted only if the caller is from a valid phone number or telecommunications channel.
SPANISH: **Llamar de vuelta**

Dial-in access controls Prevents unauthorized access from remote users that attempt to access a secured environment. These controls range from dial-back controls to remote user authentication.
SPANISH: **Controles de acceso de marcado (dial-in)**

Digital certification A process to authenticate (or certify) a party's digital signature; carried out by trusted third parties.
SPANISH: **Certificación digital**

Digital code signing The process of digitally signing computer code to ensure its integrity.
SPANISH: **Firmado digital del código**

Digital signature A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and non-repudiation. A digital signature is generated using the sender's private key or applying a one-way hash function.
SPANISH: **Firma digital**

Direct reporting engagement An engagement where management does not make a written assertion about the effectiveness of their control procedures, and the IS auditor provides an opinion about subject matter directly, such as the effectiveness of the control procedures.
SPANISH: **Contrato de reporte directo**

Disaster 1. A sudden, unplanned calamitous event causing great damage or loss. Any event that creates an inability on an organization's part to provide critical business functions for some predetermined period of time. Similar terms are business interruption, outage and catastrophe. 2. The period when organization management decides to divert from normal production responses and exercises its disaster recovery plan. Typically signifies the beginning of a move from a primary to an alternate location.
SPANISH: **Desastre**

Disaster declaration The communication to appropriate internal and external parties that the disaster recovery plan is being put into operation.
SPANISH: **Declaración de desastre**

Disaster notification fee The fee the recovery site vendor charges when the customer notifies them that a disaster has occurred and the recovery site is required. Scope Note: The fee is implemented to discourage false disaster notifications.
SPANISH: **Cargo ante notificación de desastre**

Disaster recovery Activities and programs designed to return the organization to an acceptable condition. The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions.
SPANISH: **Recuperación ante desastres**

Disaster recovery plan (DRP) A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster
SPANISH: **Plan de recuperación de desastre (DRP)**

Disaster recovery plan desk checking Typically a read-through of a disaster recovery plan without any real actions taking place. Scope Note: It generally involves a reading of the plan, discussion of the action items and definition of any gaps that might be identified.
SPANISH: **Revisión de escritorio al plan de recuperación de desastres**

Disaster recovery plan walk-through Generally a robust test of the recovery plan requiring that some recovery activities take place and are tested. A disaster scenario is often given and the recovery teams talk through the steps they would need to take to recover. As many aspects of the plan should be tested as possible.
SPANISH: **Verificación (chequeo) por medio de un recorrido del plan de recuperación de desastres**

Disaster tolerance The time gap the business can accept the non-availability of IT facilities.
SPANISH: **Tolerancia a los desastres**

Disclosure controls and procedures The processes in place designed to help ensure that all material information is disclosed by an organization in the reports it files or submits to the SEC. Scope Note: Disclosure Controls and Procedures also require that disclosures be authorized, complete and accurate, and recorded, processed, summarized and reported within the time periods specified in the SEC's rules and forms. Deficiencies in controls, as well as any significant changes to controls, must be communicated to the organization's audit committee and auditors in a timely manner. An organization's principal executive officer and financial officer must certify the existence of these controls on a quarterly basis.
SPANISH: **Controles y procedimientos de divulgación (o revelación)**

Discount rate An interest rate used to calculate a present value which might or might not include the time value of money, tax effects, risks or other factors.
SPANISH: **Tasa de descuento**

Discovery sampling A form of attribute sampling that is used to determine a specified probability of finding at least one example of an occurrence (attribute) in a population.
SPANISH: **Muestreo por descubrimiento**

Discretionary access control (DAC) A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. Scope Note: The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
SPANISH: **Control de acceso discrecional (DAC)**

Disk mirroring The practice of duplicating data in separate volumes on two hard disks to make storage more fault tolerant. Mirroring provides data protection in the case of disk failure because data are constantly updated to both disks.
SPANISH: **Duplicación (o copia espejo) de discos**

Diskless workstations A workstation or PC on a network that does not have its own disk, but instead, stores files on a network file server.
SPANISH: **Estaciones de trabajo sin disco**

Distributed data processing network A system of computers connected together by a communications network. Scope Note: Each computer processes its data and the network supports the system as a whole. Such a network enhances communication among the linked computers and allows access to shared files.
SPANISH: **Red distribuida de procesamiento de datos**

Distributed denial-of-service attack (DDoS) A denial-of-service (DoS) assault from multiple sources.
SPANISH: **Ataque distribuido de denegación de servicio (DDoS)**

Diverse routing The method of routing traffic through split cable facilities or duplicate cable facilities. Scope Note: This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and, therefore, subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises bay be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. However, acquiring this type of access is time-consuming and costly. Most carriers provide facilities for alternate and diverse routing, although the majority of services are transmitted over terrestrial media. These cable facilities are usually located in the ground or basement. Ground-based facilities are at great risk due to the aging infrastructures of cities. In addition, cable-based facilities usually share room with mechanical and electrical systems that can impose great risks due to human error and disastrous events.
SPANISH: **Enrutamiento diversificado**

Domain In COBIT, the grouping of control objectives into four logical stages in the life cycle of investments involving IT (Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate).
SPANISH: **Dominio**

Domain name system (DNS) A hierarchical database that is distributed across the Internet that allows names to be resolved into IP addresses (and vice versa) to locate services such as web and e-mail servers.
SPANISH: **Sistema de nombre de dominio (DNS)**

Domain name system (DNS) poisoning Corrupts the table of an Internet server's DNS, replacing an Internet address with the address of another vagrant or scoundrel address. Scope Note: If a Web user looks for the page with that address, the request is redirected by the scoundrel entry in the table to a different address. Cache poisoning differs from another form of DNS poisoning, in which the attacker spoofs valid e-mail accounts and floods the inboxes of administrative and technical contacts. Cache poisoning is related to URL poisoning or location poisoning, where an Internet user behavior is tracked by adding an identification number to the location line of the browser that can be recorded as the user visits successive pages on the site. Also called DNS cache poisoning or cache poisoning.
SPANISH: **Envenenamiento (o intoxicación) del sistema de nombre de dominio (DNS)**

Double-loop step Integrates the management of tactics (financial budgets and monthly reviews) and the management of strategy. Scope Note: A reporting system, based on the balanced scorecard, allows process against strategy to be monitored and corrective actions to be taken as required.
SPANISH: **Paso de doble bucle (o ciclo)**

Downloading The act of transferring computerized information from one computer to another computer.
SPANISH: **Descargando**

Downtime report A report that identifies the elapsed time when a computer is not operating correctly because of machine failure.
SPANISH: **Informe de tiempo improductivo (downtime report)**

Driver (value and risk) A driver includes an event or other activity that results in the identification of an assurance/audit need.
SPANISH: **Controlador (valor y riesgo)**

Dry-pipe fire extinguisher system Refers to a sprinkler system that does not have water in the pipes during idle usage, unlike a fully charged fire extinguisher system that has water in the pipes at all times. Scope Note: The dry-pipe system is activated at the time of the fire alarm, and water is emitted to the pipes from a water reservoir for discharge to the location of the fire.
SPANISH: **Sistema de extinción de incendios de tubería seca**

Dual control A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource, such that no single entity acting alone can access that resource.
SPANISH: **Control dual**

Due care The level of care expected from a reasonable person of similar competency under similar conditions.
SPANISH: **Debido cuidado**

Due diligence The performance of those actions that are generally regarded as prudent, responsible and necessary to conduct a thorough and objective investigation, review and/or analysis.
SPANISH: **Diligencia debida**

Due professional care Diligence that a person, who possesses a special skill, would exercise under a given set of circumstances.
SPANISH: **Debido cuidado profesional**

Dumb terminal A display terminal without processing capability. Scope Note: Dumb terminals are dependent upon the main computer for processing. All entered data are accepted without further editing or validation.
SPANISH: **Terminal tonta**

Duplex routing The method or communication mode of routing data over the communication network (also see half duplex and full duplex).
SPANISH: **Enrutamiento duplex**

Dynamic analysis Analysis that is performed in real time or in continuous form.
SPANISH: **Análisis dinámico**

Dynamic Host Configuration Protocol (DHCP) A protocol used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server. Scope Note: The DHCP server ensures that all IP addresses are unique, e.g., no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Thus IP address pool management is done by the server and not by a human network administrator.
SPANISH: **Protocolo de Configuración Dinámica del Host (DHCP)**

E

Echo checks Detects line errors by retransmitting data back to the sending device for comparison with the original transmission.
SPANISH: **Verificaciones de eco**

E-commerce The processes by which organizations conduct business electronically with their customers, suppliers and other external business partners, using the Internet as an enabling technology. Scope Note: E-commerce encompasses both business-to-business (B2B) and business-to-consumer (B2C) e-commerce models, but does not include existing non-Internet e-commerce methods based on private networks such as EDI and SWIFT.
SPANISH: **Comercio electrónico (e-commerce)**

Economic value add (EVA) Technique developed by G. Bennett Stewart III, and registered by the consulting firm of Stern, Stewart, where the performance of the corporate capital base, including depreciated investments, such as training, research and development, as well as more traditional capital investments, such as physical property and equipment, are measured against what shareholders could earn elsewhere.
SPANISH: **Valor económico agregado (EVA)**

Edit controls Detects errors in the input portion of information that is sent to the computer for processing. The controls may be manual or automated and allow the user to edit data errors before processing.
SPANISH: **Controles de edición**

Editing Ensures that data conform to predetermined criteria and enable early identification of potential errors.
SPANISH: **Edición**

Electronic data interchange (EDI) The electronic transmission of transactions (information) between two organizations. EDI promotes a more efficient paperless environment. EDI transmissions can replace the use of standard documents, including invoices or purchase orders.
SPANISH: **Intercambio electrónico de datos (EDI)**

Electronic document An administrative document (a document with legal validity, such as a contract) in any graphical representation, photographic, electromagnetic (tape) or any other type of electronic representation of the content. Scope Note: Almost all countries have developed legislation concerning the definition, use and legal validity of an electronic document. An electronic document, in whatever media that contains the data or information used as evidence of a contract or transaction between parties, is considered together with the software program capable to read it. The definition of a legally valid document as any representation of legally relevant data, not only those printed on paper, was introduced into the legislation related to computer crime. In addition, many countries in defining and disciplining the use of such instruments have issued regulations defining specifics, such as the electronic signature and data interchange formats.
SPANISH: **Documento electrónico**

Electronic funds transfer (EFT) The exchange of money via telecommunications. EFT refers to any financial transaction that originates at a terminal and transfers a sum of money from one account to another.
SPANISH: **Transferencia Electrónica de Fondos (EFT)**

Electronic signature Any technique designed to provide the electronic equivalent of a handwritten signature to demonstrate the origin and integrity of specific data. Digital signatures are an example of electronic signatures.
SPANISH: **Firma electrónica**

Electronic vaulting A data recovery strategy that allows organizations to recover data within hours after a disaster. Scope Note: Typically used for batch/journal updates to critical files to supplement full backups taken periodically, it includes recovery of data from an offsite storage media that mirrors data via a communication link.
SPANISH: **Bóvedas electrónicas de datos**

Embedded audit module (EAM) Integral part of an application system that is designed to identify and report specific transactions or other information based on pre-determined criteria. Identification of reportable items occurs as part of real-time processing. Reporting may be real-time online, or may use store and forward methods. Also known as integrated test facility or continuous auditing module.
SPANISH: **Módulos de auditoría embebidos/integrados**

Encapsulation (objects) Encapsulation is the technique used by layered protocols in which a lower-layer protocol accepts a message from a higher layer protocol and places it in the data portion of a frame in the lower layer.
SPANISH: **Encapsulado (de objetos)**

Encryption The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext).
SPANISH: **Encriptación, cifrado**

Encryption key A piece of information, in a digitized form, used by an encryption algorithm to convert the plaintext to the ciphertext.
SPANISH: **Llave/Clave de encriptación/cifrado**

End-user computing The ability of end users to design and implement their own information system utilizing computer software products.
SPANISH: **Computación de usuario final**

Engagement letter Formal document which defines the IS auditor's responsibility, authority and accountability for a specific assignment.
SPANISH: **Carta de asignación de auditoría**

Enterprise A group of individuals working together for a common purpose, typically within the context of an organizational form such as a corporation, public agency, charity or trust.
SPANISH: **Empresa**

Enterprise architecture Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support the organization's objectives.
SPANISH: **Arquitectura de la empresa**

Enterprise architecture for IT Description of the fundamental underlying design of the IT components of the business, the relationships among them, and the manner in which they support the organization's objectives.
SPANISH: **Arquitectura de la empresa para TI**

Enterprise governance A set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.
SPANISH: **Gobierno de la empresa**

Enterprise risk management (ERM) The discipline by which an enterprise in any industry assesses, controls, exploits, finances and monitors risks from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders
SPANISH: **La gestión de riesgo empresarial**

ERP (enterprise resource planning) system A packaged business software system that allows an organization to automate and integrate the majority of its business processes; share common data and practices across the entire enterprise; produce and access information in a real-time environment.
SPANISH: **Sistema ERP (planificación de los recursos de la empresa)**

Error A deviation from accuracy or correctness. Scope Note: As it relates to audit work, errors may relate to control deviations (compliance testing) or misstatements (substantive testing).
SPANISH: **Error**

Escrow agent A person, agency or organization that is authorized to act on behalf of another to create a legal relationship with a third party in regards to an escrow agreement; the custodian of an asset according to an escrow agreement. Scope Note: As it relates to a cryptographic key, an escrow agent is the agency or organization charged with the responsibility for safeguarding the key components of the unique key.
SPANISH: **Agente de depósito de fuentes (escrow)**

Escrow agreement A legal arrangement whereby an asset (often money, but sometimes other property such as art, a deed of title, web site, software source code or a cryptographic key) is delivered to a third party (called an escrow agent) to be held in trust or otherwise pending a contingency or the fulfillment of a condition or conditions in a contract. Scope Note: Upon the occurrence of the escrow agreement, the escrow agent will deliver the asset to the proper recipient; otherwise the escrow agent is bound by his/her fiduciary duty to maintain the escrow account. Source code escrow means deposit of the source code for the software into an account held by an escrow agent. Escrow is typically requested by a party licensing software (e.g., licensee or buyer), to ensure maintenance of the software. The software source code is released by the escrow agent to the licensee if the licensor (e.g., seller or contractor) files for bankruptcy or otherwise fails to maintain and update the software as promised in the software license agreement.
SPANISH: **Acuerdo de depósito de fuentes (escrow)**

Ethernet A popular network protocol and cabling scheme that uses a bus topology and CSMA/CD (carrier sense multiple access/collision detection) to prevent network failures or collisions when two devices try to access the network at the same time.
SPANISH: **Ethernet**

Event Something that happens at a specific place and/or time
SPANISH: **Evento**

Event type For the purpose of IT risk management, one of three possible sorts of events: threat event, loss event and vulnerability event. Scope Note: Being able to consistently and effectively differentiate the different types of events that contribute to risk is a critical element in developing good risk-related metrics and well-informed decisions. Unless these categorical differences are recognized and applied, any resulting metrics lose meaning and, as a result, decisions based on those metrics are far more likely to be flawed.
SPANISH: **Tipo de evento**

Evidence 1. Information that proves or disproves a stated issue 2. Information an auditor gathers in the course of performing an IS audit; relevant if it pertains to the audit objectives and has a logical relationship to the findings and conclusions it is used to support Scope Note: Audit perspective
SPANISH: **Evidencia**

Exception reports An exception report is generated by a program that identifies transactions or data that appear to be incorrect. Scope Note: Exception reports may be outside a predetermined range or may not conform to specified criteria.
SPANISH: **Informes de excepciones**

Exclusive-OR (XOR) The exclusive-OR operator returns a value of TRUE only if just one of its operands is TRUE. Scope Note: The XOR operation is a Boolean operation that produces a 0 if its two Boolean inputs are the same (0 and 0 or 1 and 1) and it produces a 1 if its two inputs are different (1 and 0). In contrast, an inclusive-OR operator returns a value of TRUE if either or both of its operands are TRUE.
SPANISH: **O exclusivo (XOR)**

Executable code The machine language code that is generally referred to as the object or load module.
SPANISH: **Código ejecutable**

Expert systems Expert systems are the most prevalent type of computer systems that arise from the research of artificial intelligence. Scope Note: An expert system has a built in hierarchy of rules, which are acquired from human experts in the appropriate field. Once input is provided, the system should be able to define the nature of the problem and provide recommendations to solve the problem.
SPANISH: **Sistemas expertos**

Exposure The potential loss to an area due to the occurrence of an adverse event.
SPANISH: **Exposición**

Extended enterprise Describes an organization that extends outside its traditional boundaries. Such organizations concentrate on the processes in which they do best and rely on someone outside the entity to perform the remaining processes.
SPANISH: **Empresa extendida**

eXtensible Markup Language (XML) Promulgated through the World Wide Web Consortium, XML is a web-based application development technique that allows designers to create their own customized tags, thus, enabling the definition, transmission, validation and interpretation of data between applications and organizations.
SPANISH: **Lenguaje de marcado extensible (Extensible Markup Language, XML)**

External router The router at the extreme edge of the network under control, usually connected to an ISP or other service provider; also known as border router.
SPANISH: **Enrutador externo**

External storage The location that contains the backup copies to be used in case recovery or restoration is required in the event of a disaster.
SPANISH: **Almacenamiento externo**

Extranet A private network that resides on the Internet and allows a company to securely share business information with customers, suppliers, or other businesses, as well as to execute electronic transactions. Scope Note: An extranet is different from an Intranet in that it is located beyond the company's firewall. Therefore, an Extranet relies on the use of securely issued digital certificates (or alternative methods of user authentication) and encryption of messages. A virtual private network (VPN) and tunneling are often used to implement Extranets, to ensure security and privacy.
SPANISH: **Extranet**

F

Fail-over The transfer of service from an incapacitated primary component to its backup component.
SPANISH: **Traspaso de la operación a su backup**

Fail-safe Describes the design properties of a computer system that allow it to resist active attempts to attack or bypass it.
SPANISH: **Resistencia ante de fallas y ataques**

Fallback procedures A plan of action or set of procedures to be performed if a system implementation, upgrade or modification does not work as intended Scope Note: Fallback procedures may involve restoring the system to its state prior to the implementation or change. Fallback procedures are needed to ensure that normal business processes continue in the event of failure and should always be considered in system migration or implementation.
SPANISH: **Procedimientos de contingencia (fallback procedures)**

Fall-through logic An optimized code based on a branch prediction that predicts which way a program will branch when an application is presented.
SPANISH: **Lógica de ramificación**

False authorization Also called false acceptance, it occurs when an unauthorized person is identified as an authorized person by the biometric system.
SPANISH: **Autorización falsa**

False enrollment Occurs when an unauthorized person manages to enroll into the biometric system. Scope Note: Enrollment is the initial process of acquiring a biometric feature and saving it as a personal reference on a smart card, a PC or in a central database.
SPANISH: **Inscripción falsa (false enrollment)**

False negative In intrusion detection, an error that occurs when an attack is misdiagnosed as a normal activity.
SPANISH: **Falso negativo**

False positive A result that has been mistakenly identified as a problem when in reality the situation is normal.
SPANISH: **Falso positivo**

Fault tolerance A system's level of resilience to seamlessly react from hardware and/or software failure.
SPANISH: **Tolerancia ante fallas**

Feasibility study A phase of a system development life cycle (SDLC) methodology that researches the feasibility and adequacy of resources for the development or acquisition of a system solution to a user need
SPANISH: **Estudio de viabilidad/factibilidad**

Fiber optic cable Glass fibers that transmit binary signals over a telecommunications network. Scope Note: Fiber optic systems have low transmission losses as compared to twisted-pair cables. They do not radiate energy or conduct electricity. They are free from corruption and lightning-induced interference, and they reduce the risk of wiretaps.
SPANISH: **Cable de fibra óptica**

Field An individual data element in a computer record. Scope Note: Examples of a field include employee name, customer address, account number, product unit price and product quantity in stock.
SPANISH: **Campo**

File A named collection of related records.
SPANISH: **Archivo**

File allocation table (FAT) A table used by the operating system to keep track of where every file is located on the disk. Scope Note: Since a file is often fragmented and thus subdivided into many sectors within the disk, the information stored in the FAT is used when loading or updating the contents of the file.
SPANISH: **Tabla de asignación de archivos (FAT)**

File layout Specifies the length of the file's record and the sequence and size of its fields. Scope Note: A file layout also will specify the type of data contained within each field. For example, alphanumeric, zoned decimal, packed and binary are types of data.
SPANISH: **Disposición de archivos (file layout)**

File server A high-capacity disk storage device or a computer that stores data centrally for network users and manages access to that data. Scope Note: File servers can be dedicated so that no process other than network management can be executed while the network is available; file servers can be non-dedicated so that standard user applications can run while the network is available.
SPANISH: **Servidor de archivos**

File Transfer Protocol (FTP) A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.).
SPANISH: **Protocolo de transferencia de archivos (FTP)**

Filtering router A router that is configured to control network access by comparing the attributes of the incoming or outgoing packets to a set of rules.
SPANISH: **Enrutador de filtrado**

FIN (Final) A flag set in a packet to indicate that this packet is the final data packet of the transmission.
SPANISH: **FIN (Final)**

Financial audit An audit designed to determine the accuracy of financial records and information.
SPANISH: **Auditoría financiera**

Finger A protocol and program that allows the remote identification of users logged into a system.
SPANISH: **Finger**

Firewall A system or combination of systems that enforces a boundary between two or more networks typically forming a barrier between a secure and an open environment such as the Internet.
SPANISH: **Cortafuegos (firewall)**

Firmware Memory chips with embedded program code that hold their content when power is turned off.
SPANISH: **Firmware**

Fiscal year Any yearly accounting period without regard to its relationship to a calendar year.
SPANISH: **Año fiscal**

Foreign key A value that represents a reference to a tuple (a row in a table) containing the matching candidate key value. Scope Note: The problem of ensuring that the database does not include any invalid foreign key values is known as the referential integrity problem. The constraint that values of a given foreign key must match values of the corresponding candidate key is known as a referential constraint. The relation (table) that contains the foreign key is referred as the referencing relation and the relations that contain the corresponding candidate key as the referenced relation or target relation. (in the relational theory it would be a candidate key, but in real DBMS implementations it is always the primary key).
SPANISH: **Clave externa**

Forensic examination The process of collecting, assessing, classifying and documenting digital evidence to assist in the identification of an offender and the method of compromise.
SPANISH: **Examinación forense**

Format checking The application of an edit, using a predefined field definition to a submitted information stream; a test to ensure that data conform to a predefined format.
SPANISH: **Verificación del formato**

Fourth-generation language (4GL) High level, user friendly, nonprocedural computer languages used to program and/or read and process computer files.
SPANISH: **Lenguaje de cuarta generación (4GL)**

Frame relay A packet-switched wide area network technology that provides faster performance than older packet-switched WAN technologies. Scope Note: Frame relay is best suited for data and image transfers. Because of its variable-length packet architecture, it is not the most efficient technology for real-time voice and video. In a frame-relay network, end nodes establish a connection via a permanent virtual circuit (PVC).
SPANISH: **Retransmisión de tramas (frame relay)**

Framework Scope Note: See control framework and IT governance framework.
SPANISH: **Marco**

Frequency A measure of the rate by which events occur over a certain period of time
SPANISH: **Frecuencia**

Function point analysis A technique used to determine the size of a development task, based on the number of function points. Scope Note: Function points are factors such as inputs, outputs, inquiries and logical internal sites.
SPANISH: **Análisis de punto de función (FPA)**

G

Gateway A device (router, firewall) on a network that serves as an entrance to another network.
SPANISH: **Pasarela (gateway)**

General computer controls Controls, other than application controls, which relate to the environment within which computer-based application systems are developed, maintained and operated, and which are therefore applicable to all applications. The objectives of general controls are to ensure the proper development and implementation of applications, the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IS strategy and an IS security policy, the organization of IS staff to separate conflicting duties and planning for disaster prevention and recovery.
SPANISH: **Controles generales de la computadora**

Generalized audit software (GAS) Multipurpose audit software that can be used for general processes, such as record selection, matching, recalculation and reporting.
SPANISH: **Software de uso generalizado en auditoría**

Generic process control A control that applies to all processes of the organization.
SPANISH: **Control de proceso genérico**

Geographic disk mirroring A data recovery strategy that takes a set of physically disparate disks and synchronously mirrors them over high performance communication lines. Any write to a disk on one side will result in a write on the other. The local write will not return until the acknowledgement of the remote write is successful.
SPANISH: **Espejamiento de discos remoto**

Geographical information system (GIS) A tool used to integrate, convert, handle, analyze and produce information regarding the surface of the earth. Scope Note: GIS data exist as maps, tridimensional virtual models, lists and tables.
SPANISH: **Sistema de información geográfica (GIS)**

Governance The oversight, direction and high-level monitoring and control of an enterprise to ensure the achievement of defined and approved objectives
SPANISH: **Gobierno (governance)**

Guideline A description of a particular way of accomplishing something that is less prescriptive than a procedure.
SPANISH: **Lineamiento**

H

Hacker An individual who attempts to gain unauthorized access to a computer system.
SPANISH: **Intruso (hacker)**

Handprint scanner A biometric device that is used to authenticate a user through palm scans.
SPANISH: **Scanner de mano**

Harden To configure a computer or other network device to resist attacks.
SPANISH: **Reforzado**

Hardware The physical components of a computer system.
SPANISH: **Hardware**

Hash function An algorithm that maps or translates one set of bits into another (generally smaller) so that a message yields the same result every time the algorithm is executed using the same message as input. Scope Note: It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm or to find two different messages that produce the same hash result using the same algorithm.
SPANISH: **Función hash**

Hash total The total of any numeric data field on a document or computer file. This total is checked against a control total of the same field to facilitate accuracy of processing.
SPANISH: **Hash total**

Help desk A service offered via phone/Internet by an organization to its clients or employees, which provides information, assistance, and troubleshooting advice regarding software, hardware, or networks. Scope Note: A help desk is staffed by people that can either resolve the problem on their own or escalate the problem to specialized personnel. A help desk is often equipped with dedicated CRM-type software that logs the problems and tracks them until they are solved.
SPANISH: **Centro de soporte (help desk)**

Heuristic filter A method often employed by antispam software to filter spam using criteria established in a centralized rule database. Scope Note: Every e-mail message is given a rank, based upon its header and contents, which is then matched against preset thresholds. A message that surpasses the threshold will be flagged as spam and discarded, returned to its sender or put in a spam directory for further review by the intended recipient.
SPANISH: **Filtro heuristic**

Hexadecimal A numbering system that uses a base of 16 and uses 16 digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E and F. Programmers use hexadecimal numbers as a convenient way of representing binary numbers.
SPANISH: **Hexadecimal**

Hierarchical database A database structured in a tree/root or parent/child relationship. Scope Note: In a hierarchical database, each parent can have many children, but each child may have only one parent.
SPANISH: **Base de datos jerárquica**

Honeypot A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems. Scope Note: Also known as "decoy server".
SPANISH: **Honeypot**

Hot site A fully operational offsite data processing facility equipped with both hardware and system software to be used in the event of a disaster.
SPANISH: **Hot site**

Hub A common connection point for devices in a network, hubs commonly are used to connect segments of a LAN. Scope Note: A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
SPANISH: **Concentrador (hub)**

Hurdle rate Also known as required rate of return; Required rate of return, above which an investment makes sense and below which it does not. Scope Note: Hurdle rate is often based on the cost of capital, plus or minus a risk premium, and often varied based upon prevailing economic conditions.
SPANISH: **Tasa de retorno mínima aceptable**

Hybrid application controls Those controls that consist of a combination of manual and automated activities, all of which must operate for the control to be effective. Scope Note: Sometimes referred to as computer-dependent application controls.
SPANISH: **Controles híbridos de aplicación**

Hyperlink An electronic pathway that may be displayed in the form of highlighted text, graphics or a button that connects one web page with another web page address.
SPANISH: **Hipervínculo**

Hypertext A language, which enables electronic documents that present information that can be connected together by links instead of being presented sequentially, as is the case with normal text.
SPANISH: **Hipertexto**

Hypertext Markup Language (HTML) A language designed for the creation of web pages with hypertext and other information to be displayed in a web browser; used to structure information--denoting certain text as headings, paragraphs, lists and so on--and can be used to describe, to some degree, the appearance and semantics of a document.
SPANISH: **Lenguaje de marcado de hipertexto (HTML)**

Hypertext Transfer Protocol Secure (HTTPS) A protocol for accessing a secure web server, whereby all data transferred is encrypted.
SPANISH: **Protocolo seguro de transferencia de hipertexto (HTTPS)**

Hypertext Transfer Protocol (HTTP) A communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML, XML or other pages to the client browsers.
SPANISH: **Protocolo de transferencia de hipertexto (HTTP)**

I

Idle standby A fail-over process in which the primary node owns the resource group. The backup node runs idle, only supervising the primary node. Scope Note: In case of a primary node outage, the backup node takes over. The nodes are prioritized, which means the surviving node with the highest priority will acquire the resource group. A higher priority node joining the cluster will thus cause a short service interruption.
SPANISH: **Modo de espera inactivo**

IEEE Pronounced I-triple-E, IEEE (Institute of Electrical and Electronics Engineers) is an organization composed of engineers, scientists and students. Scope Note: The IEEE is best known for developing standards for the computer and electronics industry.
SPANISH: **IEEE**

Image processing The process of electronically inputting source documents by taking an image of the document, thereby eliminating the need for key entry.
SPANISH: **Procesamiento de imágenes**

Impact analysis A study to prioritize the criticality of information resources for the organization based on costs (or consequences) of adverse events.
an impact analysis, threats to assets are identified and potential business losses determined for different time periods. This assessment is used to justify the extent of safeguards that are required and recovery time frames. This analysis is the basis for establishing the recovery strategy.
SPANISH: **Análisis de impacto**

Impact assessment A review of the possible consequences of a risk. Scope Note: See impact analysis.
SPANISH: **Valoración del impacto**

Impersonation As a security concept related to Windows NT, allows a server application to temporarily "be" the client in terms of access to secure objects. Scope Note: Impersonation has three possible levels: identification, letting the server inspect the client's identity; impersonation, letting the server act on behalf of the client; and delegation, the same as impersonation but extended to remote systems to which the server connects (through the preservation of credentials). Impersonation by imitating or copying the identification, behavior or actions of another may also be used in social engineering to obtain otherwise unauthorized physical access.
SPANISH: **Suplantación de identidad**

Implement In business, includes the full economic life cycle of the investment program through retirement, i.e., when the full expected value of the investment is realized, as much value as is deemed possible has been realized, or it is determined that the expected value cannot be realized and the program is terminated.
SPANISH: **Implementar**

Implementation life cycle review Refers to the controls that support the process of transformation of the organization's legacy information systems into the ERP applications. Scope Note: Implementation life cycle review would largely cover all aspects of systems implementation and configuration, such as change management
SPANISH: **Revisión del ciclo de vida de la implementación**

Incident Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service.
SPANISH: **Incidente**

Incident response The response of an organization to a disaster or other significant event that may significantly affect the organization, its people, or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan, performing damage assessment, and any other measures necessary to bring an organization to a more stable status.
SPANISH: **Respuesta a incidentes**

Incremental testing Deliberately testing only the value-added functionality of a software component.
SPANISH: **Pruebas incrementales**

Independence 1. Self-governance. 2. Freedom from conflict of interest and undue influence. Scope Note: The IS auditor should be free to make his/her own decisions, not influenced by the organization being audited and its people (managers and employers).
SPANISH: **Independencia**

Independent appearance The outward impression of being self-governing and free from conflict of interest and undue influence.
SPANISH: **Apariencia independiente**

Independent attitude Impartial point of view which allows the IS auditor to act objectively and with fairness.
SPANISH: **Actitud independiente**

Indexed Sequential Access Method (ISAM) A disk access method that stores data sequentially while also maintaining an index of key fields to all the records in the file for direct access capability
SPANISH: **Método de acceso secuencial indexado (ISAM)**

Indexed sequential file A file format in which records are organized and can be accessed, according to a pre-established key that is part of the record.
SPANISH: **Archivo secuencial indexado**

Information architecture Information architecture is one component of IT architecture (together with applications and technology).
SPANISH: **Arquitectura de la información**

Information criteria Attributes of information that must be satisfied to meet business requirements.
SPANISH: **Criterios de la información**

Information engineering Data-oriented development techniques that work on the premise that data are at the center of information processing and that certain data relationships are significant to a business and must be represented in the data structure of its systems.
SPANISH: **Ingeniería de la información**

Information processing facility (IPF) The computer room and support areas.
SPANISH: **Infraestructura para el procesamiento de información (IPF)**

Information security Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability).
SPANISH: **Seguridad de la información**

Information security governance The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.
SPANISH: **Gobierno de la seguridad de la información**

Information security program The overall combination of technical, operational and procedural measures, and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis.
SPANISH: **Programa de seguridad de la información**

Information systems (IS) The combination of strategic, managerial and operational activities involved in the gathering, processing, storage, distributing, and use of information and its related technologies. Scope Note: Information systems are distinct from information technology (IT) in that an information system has an IT component that interacts with the process components.
SPANISH: **Sistemas de información (SI)**

Information technology (IT) The hardware, software, communications and other facilities used to input, store, process, transmit and output data in whatever form.
SPANISH: **Tecnología de la información (TI)**

Informed In a RACI chart, refers to those people who are kept up to date on the progress of an activity (one-way communication).
SPANISH: **Informado**

Inherent risk 1. The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls) 2. The risk that a material error could occur, assuming that there are no related internal controls to prevent or detect the error Scope Note: Audit perspective; also see control risk.
SPANISH: **Riesgo inherente**

Inheritance (objects) Database structures that have a strict hierarchy (no multiple inheritance). Inheritance can initiate other objects irrespective of the class hierarchy, thus there is no strict hierarchy of objects.
SPANISH: **Herencia (objetos) (inheritance)**

Initial program load (IPL) The initialization procedure that causes an operating system to be loaded into storage at the beginning of a workday or after a system malfunction.
SPANISH: **Carga inicial de programas (IPL)**

Initialization vector (IV) collisions A major concern is in the way WEP allocates the RC4 Initialization Vectors (IVs) used to create the keys that are used to drive a pseudo random number generator that is eventually used for encryption of the wireless data traffic. The IV in WEP is a 24-bit field—a small space that practically guarantees reuse, resulting in key reuse. The WEP standard also fails to specify how these IVs are assigned. Many wireless network cards reset these IVs to zero and then increment them by one for every use. If an attacker can capture two packets using the same IV (the same key if the key has not been changed), mechanisms can be used to determine portions of the original packets. This and other weaknesses result in key reuse, resulting in susceptibility to attacks to determine the keys used. These attacks require a large number of packets (5-6 million) to actually fully derive the WEP key, but on a large, busy network this can occur in a short time, perhaps in as quickly as 10 minutes (although, even some of the largest corporate networks will likely require much more time than this to gather enough packets). In WEP protected wireless networks, many times multiple, or all, stations use the same shared key. This increases the chances of IV collisions greatly. The result of this is that the network becomes insecure if the WEP keys are not changed often. This furthers the need for a WEP key management protocol.
SPANISH: **Colisiones del vector de inicialización (VI)**

Input controls Techniques and procedures used to verify, validate and edit data, to ensure that only correct data are entered into the computer.
SPANISH: **Controles de entrada**

Instant messaging An online mechanism or a form of real-time communication between two or more people based on typed text and multimedia data. Scope Note: Instant messaging text is conveyed via computers or another electronic device (e.g., cell phone or PDA) connected over a network, such as the Internet.
SPANISH: **Mensajería instantánea**

Integrated services digital network (ISDN) A public end-to-end digital telecommunications network with signaling, switching and transport capabilities supporting a wide range of service accessed by standardized interfaces with integrated customer control. Scope Note: The standard allows transmission of digital voice, video and data over 64 Kpbs lines.
SPANISH: **Red digital de servicios integrados (RDSI / ISDN).**

Integrated test facilities (ITF) A testing methodology where test data are processed in production systems. Scope Note: The data usually represent a set of fictitious entities such as departments, customers and products. Output reports are verified to confirm the correctness of the processing.
SPANISH: **Utilidad integrada de prueba (ITF, integrated test facility)**

Integrity The accuracy, completeness and validity of information.
SPANISH: **Integridad**

Interface testing A testing technique that is used to evaluate output from one application, while the information is sent as input to another application.
SPANISH: **Pruebas de interfaz**

Internal control The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected
SPANISH: **Control interno**

Internal control environment The relevant environment on which the controls have effect.
SPANISH: **Entorno del control interno**

Internal control over financial reporting A process designed by, or under the supervision of, the registrant's principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principals and includes those policies and procedures that:
Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant
Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the registrant
Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements.
SPANISH: **Control interno sobre los informes financieros**

Internal control structure The dynamic, integrated processes, effected by the governing body, management and all other staff, that are designed to provide reasonable assurance regarding the achievement of the following general objectives:
Effectiveness, efficiency and economy of operations
Reliability of management
Compliance with applicable laws, regulations and internal policies's strategies for achieving these general objectives are affected by the design and operation of the following components:
Control environment
Information system
Control procedures
SPANISH: **Estructura del control interno**

Internal penetrators Authorized users of a computer system who overstep their legitimate access rights. Scope Note: This category is divided into masqueraders and clandestine users.
SPANISH: **Atacantes internos**

Internal rate of return (IRR) The discount rate that equates an investment cost with its projected earnings. Scope Note: When discounted at the IRR, the present value of the cash outflow will equal the present value of the cash inflow. The IRR and NPV are measures of the expected profitability of an project.
SPANISH: **Tasa interna de retorno (IRR)**

Internal storage The main memory of the computer's central processing unit.
SPANISH: **Almacenamiento interno**

Internet 1. Two or more networks connected by a router 2. The world's largest network using TCP/IP protocols to link government, university and commercial institutions.
SPANISH: **Internet**

Internet banking Use of the Internet as a remote delivery channel for banking services. Scope Note: Services include the traditional ones, such as opening an account or transferring funds to different accounts, and new banking services, such as electronic bill presentment and payment (allowing customers to receive and pay bills on a bank's web site).
SPANISH: **Banca por Internet**

Internet Control Message Protocol (ICMP) A set of protocols that allow systems to communicate information about the state of services on other systems. Scope Note: For example, ICMP is used in determining whether systems are up, maximum packet sizes on links, whether a destination host/network/port is available. Hackers typically (abuse) use ICMP to determine information about the remote site.
SPANISH: **Protocolo de mensajes de control de Internet (ICMP)**

Internet Engineering Task Force (IETF) The Internet standards setting organization with affiliates internationally from network industry representatives. This includes all network industry developers and researchers concerned with evolution and planned growth of the Internet.
SPANISH: **Grupo de trabajo de ingeniería de Internet (IETF)**

Internet Inter-ORB Protocol (IIOP) A protocol developed by the object management group (OMG) to implement Common Object Request Broker Architecture (CORBA) solutions over the World Wide Web. Scope Note: CORBA enables modules of network-based programs to communicate with one another. These modules or program parts, such as tables, arrays, and more complex program sub elements, are referred to as objects. Use of IIOP in this process enables browsers and servers to exchange both simple and complex objects. This significantly differs from HTTP, which only supports the transmission of text.
SPANISH: **Protocolo Inter-ORB de Internet (IIOP)**

Internet packet (IP) spoofing An attack using packets with the spoofed source Internet packet (IP) addresses. Scope Note: This technique exploits applications that use authentication based on IP addresses. This technique also may enable an unauthorized user to gain root access on the target system.
SPANISH: **Suplantación de IP (IP spoofing)**

Internet protocol (IP) Specifies the format of packets and the addressing scheme.
SPANISH: **Internet Protocol (IP)**

Internet Protocol Security (IPSec) A set of protocols developed by the IETF to support the secure exchange of packets.
SPANISH: **Seguridad del protocolo de Internet (IPSec)**

Internet service provider (ISP) A third party that provides individuals and organizations access to the Internet and a variety of other Internet-related services.
SPANISH: **Proveedor de servicios de Internet (Internet service provider, ISP)**

Interruption window The time the company can wait from the point of failure to the restoration of the minimum and critical services or applications. After this time, the progressive losses caused by the interruption are excessive for the organization.
SPANISH: **Ventana de interrupción**

Intranet A private network that uses the infrastructure and standards of the Internet and World Wide Web, but is isolated from the public Internet by firewall barriers.
SPANISH: **Intranet**

Intrusion Any event where unauthorized access occurs.
SPANISH: **Intrusión**

Intrusion detection The process of monitoring the events occurring in a computer system or network to detect signs of unauthorized access or attack.
SPANISH: **Detección de intrusos**

Intrusion detection system (IDS) An IDS inspects network and host security activity to identify suspicious patterns that may indicate a network or system attack.
SPANISH: **Sistema de detección de intrusos**

Intrusive monitoring In vulnerability analysis, gaining information by performing checks that affects the normal operation of the system, even crashing the system.
SPANISH: **Monitoreo intrusivo**

Irregularity Intentional violation of established management policy or regulatory requirement. It may consist of deliberate misstatements or omission of information concerning the area under audit or the organization as a whole, gross negligence or unintentional illegal acts.
SPANISH: **Irregularidad**

ISO 27001 Information Security Management—Specification with Guidance for Use; the replacement for BS7799-2. It is intended to provide the foundation for third-party audit and is harmonized with other management standards, such as ISO/IEC 9001 and 14001.
SPANISH: **ISO 27001**

ISO 9001:2000 Code of practice for quality management from the International Organization for Standardization (ISO). ISO 9001:2000, which specifies requirements for a quality management system for any organization that needs to demonstrate its ability to consistently provide product or service that meets particular quality targets.
SPANISH: **ISO 9001:2000**

ISO/IEC 17799 This standard defines information's confidentiality, integrity and availability controls in a comprehensive information security management system. Scope Note: Originally released as part of the British Standard for Information Security in 1999 and then as the Code of Practice for Information Security Management in October 2000, it was elevated by the International Organization for Standardization (ISO) to an international code of practice for information security management. The latest version is ISO/IEC 17799:2005.
SPANISH: **ISO/IEC 17799**

IT architecture Description of the fundamental underlying design of the IT components of the business, the relationships among them, and the manner in which they support the organization's objectives
SPANISH: **Arquitectura de TI**

IT governance The responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives.
SPANISH: **Gobierno de TI**

IT governance framework A model that integrates a set of guidelines, policies and methods that represent the organizational approach to the IT governance Scope Note: Per COBIT 4.0, IT governance is the responsibility of the board of directors and executive management. It is an integral part of institutional governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives.
SPANISH: **Marco de gobierno de TI**

IT Governance Institute (ITGI) Founded by the Information Systems Audit and Control Association and it affiliated foundation in 1998, ITGI strives to assist enterprise leadership in ensuring long-term, sustainable enterprise success and increase stakeholder value by expanding awareness.
SPANISH: **IT Governance Institute (ITGI)**

IT incident Any event that is not part of the ordinary operation of a service that causes, or may cause, an interruption to, or a reduction in, the quality of that service.
SPANISH: **Incidente de TI**

IT infrastructure The set of hardware, software and facilities that integrates an organization's IT assets Scope Note: Specifically, the equipment (including servers, routers, switches, and cabling), software, services and products used in storing, processing, transmitting and displaying all forms of information for the organization's users
SPANISH: **Infraestructura de TI**

IT investment dashboard A tool for setting expectations for an organization at each level and continuous monitoring of the performance against set targets for expenditures on and returns from IT-enabled investment projects in terms of business values.
SPANISH: **Cuadro de mando para la inversión en TI**

IT risk The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise
SPANISH: **Riesgo de TI**

IT risk issue 1. An instance of an IT risk 2. A combination of control, value and threat conditions that impose a noteworthy level of IT risk
SPANISH: **Problema de riesgo de TI**

IT risk profile A description of the overall (identified) IT risk to which the enterprise is exposed
SPANISH: **Perfil de riesgo de TI**

IT risk register A repository of the key attributes of potential and known IT risk issues
may include name, description, owner, expected/actual frequency, potential/actual magnitude, potential/actual business impact, disposition.
SPANISH: **Registro de riesgos de TI**

IT risk scenario The description of an IT-related event that can lead to a business impact
SPANISH: **Escenario de riesgos de TI**

IT steering committee An executive management level committee that assists the executive in the delivery of the IT strategy, oversees day-to-day management of IT service delivery and IT projects and focuses on implementation aspects.
SPANISH: **Comité de dirección de TI**

IT strategic plan A long-term plan, i.e., three- to five-year horizon, in which business and IT management cooperatively describe how IT resources will contribute to the enterprise's strategic objectives (goals).
SPANISH: **Plan estratégico de TI**

IT strategy committee Committee at the level of the board of directors to ensure that the board is involved in major IT matters/decisions. Scope Note: The committee is primarily accountable for managing the portfolios of IT-enabled investments, IT services and other IT resources. The committee is the owner of the portfolio.
SPANISH: **Comité de estrategia de TI**

IT tactical plan A medium-term plan, i.e., six- to 18-month horizon, that translates the IT strategic plan direction into required initiatives, resource requirements and ways in which resources and benefits will be monitored and managed.
SPANISH: **Plan táctico de TI**

IT user A person who uses IT to support or achieve a business objective.
SPANISH: **Usuario de TI**

ITIL The UK Office of Government Commerce (OGC) IT Infrastructure Library. A set of guides on the management and provision of operational IT services.
SPANISH: **ITIL**

IT-related incident An IT-related event that causes an operational, developmental and/or strategic business impact
SPANISH: **Incidente relacionado con TI**

J

Job control language (JCL) A language used to control run routines in connection with performing tasks on a computer.
SPANISH: **Lenguaje para el control de trabajos (JCL)**

Journal entry A debit or credit to a general ledger account, in Oracle. See also manual journal entry.
SPANISH: **Entrada en libros diarios**

Judgment sampling Any sample that is selected subjectively or in such a manner that the sample selection process is not random or the sampling results are not evaluated mathematically.
SPANISH: **Muestreo basado en juicio**

K

Key goal indicators (KGIs) Measures that tell management, after the fact, whether an IT process has achieved its business requirements, usually expressed in terms of information criteria.
SPANISH: **Indicadores clave de metas (KGI)**

Key management practices Those management practices required to successfully execute business processes.
SPANISH: **Prácticas clave de administración del negocio**

Key performance indicator (KPI) A measure that determine how well the process is performing in enabling the goal to be reached. Scope Note: A KPI is a lead indicator of whether a goal will likely be reached, and a good indicator of capability, practices and skills. It measures an activity goal, which is an action the process owner must take to achieve effective process performance.
SPANISH: **Indicador clave de desempeño (KPI)**

Key risk indicator (KRI) A subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk. Scope Note: See risk indicator.
SPANISH: **Indicador clave de riesgo (KRI)**

Knowledge portal Refers to the repository of a core of information and knowledge for the extended enterprise. Scope Note: This is generally a web-based implementation containing a core repository of information provided for the extended enterprise to resolve any issues.
SPANISH: **Portal de conocimientos**

L

Latency The time it takes a system and network delay to respond. Scope Note: More specifically, system latency is the time a system takes to retrieve data. Network latency is the time it takes for a packet to travel from source to the final destination.
SPANISH: **Latencia**

Leadership The ability and process to translate vision into desired behaviors that are followed at all levels of the extended enterprise.
SPANISH: **Liderazgo**

Leased lines A communication line permanently assigned to connect two points, as opposed to a dial-up line that is only available and open when a connection is made by dialing the target machine or network. Also known as a dedicated line.
SPANISH: **Líneas arrendadas**

Level of assurance Refers to the degree to which the subject matter has been examined or reviewed.
SPANISH: **Nivel de aseguramiento**

Librarian The individual responsible for the safeguard and maintenance of all program and data files.
SPANISH: **bibliotecario (librarian)**

Licensing agreement A contract that establishes the terms and conditions under which a piece of software is being licensed (i.e., made legally available for use) from the software developer (owner) to the user.
SPANISH: **Acuerdo de licencia**

Life cycle A series of stages that characterize the course of existence of an organizational investment (e.g., product, project, program).
SPANISH: **Ciclo de vida**

Limit check Tests of specified amount fields against stipulated high or low limits of acceptability. Scope Note: When both high and low values are used, the test may be called a range check.
SPANISH: **Verificación de límites**

Link editor (linkage editor) A utility program that combines several separately compiled modules into one, resolving internal references between them.
SPANISH: **Editor de vínculos (link editor)**

Literals Any notation for representing a value within programming language source code, e.g., a string literal; a chunk of input data that is represented "as is" in compressed data.
SPANISH: **Literales**

Local area network (LAN) Communications networks that serve several users within a specified geographical area. Scope Note: Personal computer LANs function as distributed processing systems in which each computer in the network does its own processing and manages some of its data. Shared data are stored in a file server that acts as a remote disk drive for all users in the network.
SPANISH: **Red de área local (LAN)**

Log To record details of information or events in an organized record-keeping system, usually sequenced in the order they occurred.
SPANISH: **Registro (log)**

Logical access controls The policies, procedures, organizational structure and electronic access controls designed to restrict access to computer software and data files.
SPANISH: **Controles de acceso lógico**

Logoff Disconnecting from the computer.
SPANISH: **Finalización de sesión (logoff)**

Logon The act of connecting to the computer, which typically requires entry of a user ID and password into a computer terminal.
SPANISH: **Inicio de sesión (logon)**

Logs/log file Files created specifically to record various actions occurring on the system to be monitored, such as failed login attempts, full disk drives and e-mail delivery failures.
SPANISH: **Bitácora/archivo de registros de log**

Loss event Any event where a threat event results in loss Scope Note: From Jones, J.; "FAIR Taxonomy," Risk Mgmt Insight, USA, 2008
SPANISH: **Pérdida ante evento**

M

Machine language The logical language a computer understands.
SPANISH: **Lenguaje de máquina**

Magnetic card reader A card reader that reads cards with a magnetic surface on which data can be stored and retrieved.
SPANISH: **Lector de tarjetas magnéticas**

Magnetic ink character recognition (MICR) Used to electronically input, read and interpret information directly from a source document. Scope Note: MICR requires the source document to have specially-coded magnetic ink typeset
SPANISH: **Reconocimiento de caracteres de tinta magnética (MICR)**

Magnitude A measure of the potential severity of loss or the potential gain from realized events/scenarios
SPANISH: **Magnitud**

Mail relay server An e-mail server that relays messages so that neither the sender nor the recipient is a local user.
SPANISH: **Servidor de retransmisión/intermediador de correo**

Malware Short for "malicious software", malware is software designed to infiltrate, damage or obtain information from a computer system without the owner's consent. Scope Note: Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and adware. Spyware is generally used for marketing purposes and, as such, not really malicious although it is generally unwanted. However, spyware can also be used to gather information for identity theft or other clearly illicit purposes.
SPANISH: **Software malintencionado (malware)**

Management information system (MIS) An organized assembly of resources and procedures required to collect, process and distribute data for use in decision making.
SPANISH: **Sistema de información gerencial (MIS)**

Mandatory access control (MAC) A means of restricting access to data based on varying degrees of security requirements for information contained in the objects and the corresponding security clearance of users or programs acting on their behalf.
SPANISH: **Control de acceso obligatorio (MAC)**

Man-in-the-middle attack An attack strategy in which the attacker intercepts the communications stream between two parts of the victim system and then replaces the traffic between the two components with the intruder's own, eventually assuming control of the communication.
SPANISH: **Ataque de "hombre en el medio"**

Manual journal entry A journal entry entered at a computer terminal. Scope Note: Manual journal entries can include regular, statistical, inter-company and foreign currency entries
SPANISH: **Entrada manual en libros diarios**

Mapping Diagramming data that are to be exchanged electronically, including how it is to be used and what business management systems need it. Also see application tracing and mapping. Scope Note: Mapping is a preliminary step for developing an applications link.
SPANISH: **Mapeo (mapping)**

Masking A computerized technique of blocking out the display of sensitive information, such as passwords, on a computer terminal or report.
SPANISH: **Enmascaramiento (masking)**

Masqueraders Attackers that penetrate systems by using the identity of legitimate users and their logon credentials.
SPANISH: **Atacantes que suplantan/secuestran identidades**

Master file A file of semi permanent information that is used frequently for processing data or for more than one purpose.
SPANISH: **Archivo maestro**

Materiality An auditing concept regarding the importance of an item of information with regard to its impact or effect on the functioning of the entity being audited. An expression of the relative significance or importance of a particular matter in the context of the organization as a whole.
SPANISH: **Materialidad**

Maturity In business, indicates the degree of reliability or dependency the business can place on a process achieving the desired goals or objectives
SPANISH: **Madurez**

Maturity model Scope Note: See capability maturity model (CMM).
SPANISH: **Modelo de madurez**

Maximum tolerable outages (MTO) Maximum time the organization can support processing in alternate mode.
SPANISH: **Máximo tiempo tolerable de Interrupción (MTOs)**

Measure A standard used to evaluate and communicate performance against expected results. Scope Note: Measures are normally quantitative in nature capturing numbers, dollars, percentages, etc., but can also address qualitative information such as customer satisfaction. Reporting and monitoring measures help an organization gauge progress toward effective implementation of strategy.
SPANISH: **Medida**

Media access control (MAC) Applied to the hardware at the factory and cannot be modified, MAC is a unique, 48-bit, hard-coded address of a physical layer device, such as an Ethernet LAN or a wireless network card.
SPANISH: **Control de acceso al medio (MAC)**

Media oxidation The deterioration of the media upon which data is digitally stored due to exposure to oxygen and moisture. Scope Note: Tapes deteriorating in a warm, humid environment are an example of media oxidation. Proper environmental controls should prevent, or significantly slow, this process.
SPANISH: **Oxidación de medios/soportes**

Memory dump The act of copying raw data from one place to another with little or no formatting for readability. Scope Note: Usually, dump refers to copying data from main memory to a display screen or a printer. Dumps are useful for diagnosing bugs. After a program fails, one can study the dump and analyze the contents of memory at the time of the failure. Dumps are usually output in a difficult-to-read form (that is, binary, octal or hexadecimal), so a memory dump will not help unless each person knows exactly for what to look.
SPANISH: **Volcado/Vuelco de memoria (memory dump)**

Message authentication code An ANSI standard checksum that is computed using Data Encryption Standard (DES).
SPANISH: **Código de autenticación de mensajes**

Message switching A telecommunications traffic controlling methodology in which a complete message is sent to a concentration point and stored until the communications path is established.
SPANISH: **Conmutación de mensajes**

Metric Specific descriptions of how a quantitative and periodic assessment of performance is to be measured. Scope Note: A complete metric defines the unit used, frequency, ideal target value, the procedure to carry out the measurement and the procedure for the interpretation of the assessment.
SPANISH: **Métrica**

Microwave transmission A high-capacity line-of-sight transmission of data signals through the atmosphere which often requires relay stations.
SPANISH: **Transmisión por microondas**

Middleware Another term for an application programmer interface (API). It refers to the interfaces that allow programmers to access lower- or higher-level services by providing an intermediary layer that includes function calls to the services.
SPANISH: **Middleware**

Milestone A terminal element that marks the completion of a work package or phase. Scope Note: Typically marked by a high-level event such as project completion, receipt, endorsement or signing of a previously-defined deliverable or a high-level review meeting at which the appropriate level of project completion is determined and agreed to, a milestone is associated with some sort of decision that outlines the future of a project and, for outsourced project, may have a payment to the contractor associated with it.
SPANISH: **Objetivo**

Mirrored site An alternate site that contains the same information as the original. Scope Note: Mirror sites are set up for backup and disaster recovery as well as to balance the traffic load for numerous download requests. Such download mirrors are often placed in different locations throughout the Internet.
SPANISH: **Sitio espejo**

Mission-critical application An application that is vital to the operation of the organization. The term is very popular for describing the applications required to run the day-to-day business.
SPANISH: **Aplicación de misión crítica (mission-critical application)**

Misuse detection Detection on the basis of whether the system activity matches that defined as bad.
SPANISH: **Detección ante uso indebido/inesperado**

Mobile computing Extends the concept of wireless computing to devices that enable new kinds of applications and expand an enterprise network to reach places in circumstances that could never have been done by other means. Scope Note: Mobile computing is comprised of PDAs, cellular phones, laptops and other technologies of this kind.
SPANISH: **Dispositivos de computación móvil**

Mobile site The use of a mobile/temporary facility to serve as a business resumption location. They can usually be delivered to any site and can house information technology and staff.
SPANISH: **Sitio móvil**

Modeling Developing a simplified representation of a system or phenomenon. Scope Note: Such representations may be static or dynamic, in which case behavior of the system or phenomenon under different conditions can be simulated.
SPANISH: **Modelaje**

MODEM (modulator/demodulator) Connects a terminal or computer to a communications network via a telephone line. Modems turn digital pulses from the computer into frequencies within the audio range of the telephone system. When acting in the receiver capacity, a modem decodes incoming frequencies.
SPANISH: **Modem (modulador-desmodulador)**

Modulation The process of converting a digital computer signal into an analog telecommunications signal.
SPANISH: **Modulación**

Monetary unit sampling A sampling technique that estimates the amount of overstatement in an account balance.
SPANISH: **Muestreo de unidad monetaria**

Monitoring policy Rules outlining or delineating the way in which information about the use of computers, networks, applications and information is captured and interpreted.
SPANISH: **Política de seguimiento**

Multiplexor A device used for combining several lower-speed channels into a higher-speed channel.
SPANISH: **Multiplexor**

Mutual takeover A fail-over process, which is basically a two-way idle standby: two servers are configured so that both can take over the other node's resource group. Both must have enough CPU power to run both applications with sufficient speed, or performance losses must be taken into account expected until the failed node reintegrates.
SPANISH: **Recuperación cruzada ante contingencia**

N

Net present value (NPV) Calculated by using an after-tax discount rate of an investment and a series of expected incremental cash outflows (the initial investment and operational costs) and cash inflows (cost savings or revenues) that occur at regular periods during the life cycle of the investment. Scope Note: To arrive at a fair NPV calculation, cash inflows accrued by the business up to about five years after project deployment should be taken into account as well.
SPANISH: **Valor presente neto (NPV)**

Net return The revenue after tax and other deductions that a project or business makes. Often also classified as net profit.
SPANISH: **Ganancia neta**

Netcat A simple UNIX utility, which reads and writes data across network connections using TCP or UDP protocols. It is designed to be a reliable back-end tool that can be used directly or is easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection needed and has several interesting built-in capabilities. Netcat is now part of the Red Hat Power Tools collection and comes standard on SuSE Linux, Debian Linux, NetBSD and OpenBSD distributions.
SPANISH: **Netcat**

Net-centric technologies The contents and security of information or objects (software and data) on the network are now of prime importance compared with traditional computer processing that emphasizes the location of hardware and its related software and data. Scope Note: An example of net-centric technologies is the Internet, where the network is its primary concern.
SPANISH: **Tecnologías Net-Centric**

Netware A popular local area network operating system developed by the Novell Corp.
SPANISH: **Netware**

Network A system of interconnected computers and the communications equipment used to connect them.
SPANISH: **Red**

Network administrator Responsible for planning, implementing and maintaining the telecommunications infrastructure, and also may be responsible for voice networks. Scope Note: For smaller organizations, the network administrator may also maintain a LAN and assist end users.
SPANISH: **Administrador de la red**

Network attached storage (NAS) Utilizes dedicated storage devices that centralizes storage of data. Scope Note: Network attached storage devices generally do not provide traditional file/print or application services.
SPANISH: **Almacenamiento conectado en red (NAS)**

Network hop An attack strategy in which the attacker successively hacks into a series of connected systems, obscuring his/her identify from the victim of the attack.
SPANISH: **Salto de red**

Network interface card (NIC) A communications card that when inserted into a computer, allows it to communicate with other computers on a network. Scope Note: Most network interface cards are designed for a particular type of network or protocol.
SPANISH: **tarjeta de interfaz de red (NIC)**

Node Point at which terminals are given access to a network.
SPANISH: **Nodo**

Noise Disturbances, such as static, in data transmissions that cause messages to be misinterpreted by the receiver.
SPANISH: **Ruido**

Nondisclosure agreement (NDA) A legal contract between at least two parties that outlines confidential materials the parties wish to share with one another for certain purposes, but wish to restrict from generalized use; a contract through which the parties agree not to disclose information covered by the agreement. Scope Note: Also called a confidential disclosure agreement (CDA), confidentiality agreement or secrecy agreement. An NDA creates a confidential relationship between the parties to protect any type of trade secret. As such, an NDA can protect non-public business information. In the case of certain governmental entities, the confidentiality of information other than trade secrets may be subject to applicable statutory requirements, and in some cases may be required to be revealed to an outside party requesting the information. Generally, the governmental entity will include a provision in the contract to allow the seller to review a request for information the seller identifies as confidential and the seller may appeal such a decision requiring disclosure. NDAs are commonly signed when two companies or individuals are considering doing business together and need to understand the processes used in one another's businesses solely for the purpose of evaluating the potential business relationship. NDAs can be "mutual," meaning both parties are restricted in their use of the materials provided, or they can only restrict a single party. It is also possible for an employee to sign an NDA or NDA-like agreement with a company at the time of hiring; in fact, some employment agreements will include a clause restricting "confidential information" in general.
SPANISH: **Acuerdo de no divulgación (NDA)**

Nonintrusive monitoring The use of transported probes or traces to assemble information, track traffic and identify vulnerabilities.
SPANISH: **Monitoreo no intrusivo**

Nonrepudiable transactions Transactions that cannot be denied after the fact..
SPANISH: **Transacciones no repudiables**

Nonrepudiation The assurance that a party cannot later deny originating data; provision of proof of the integrity and origin of the data and can be verified by a third party. Scope Note: A digital signature can provide non-repudiation.
SPANISH: **No repudio**

Normalization The elimination of redundant data.
SPANISH: **Normalización**

Numeric check An edit check designed to ensure the data in a particular field is numeric.
SPANISH: **Verificación numérica**

O

Object code Machine-readable instructions produced from a compiler or assembler program that has accepted and translated the source code.
SPANISH: **Código objeto**

Object management group (OMG) A consortium with more than 700 affiliates from the software industry whose purpose is to provide a common framework for developing applications using object-oriented programming techniques. Scope Note: For example, OMG is known principally for promulgating the CORBA specification.
SPANISH: **Grupo de gestión de objetos (OMG)**

Object orientation An approach to system development where the basic unit of attention is an object, which represents an encapsulation of both data (an object's attributes) and functionality (an object's methods). Scope Note: Objects usually are created using a general template called a class. Classes are the basis for most design work in objects. Classes and their objects communicate in defined ways. Aggregate classes interact through messages, which are directed requests for services from one class (the client) to another class (the server). A class may share the structure or methods defined in one or more other classes--a relationship known as inheritance.
SPANISH: **Orientación a objetos**

Objectivity The ability to exercise judgment, express opinions and present recommendations with impartiality
SPANISH: **Objetividad**

Object-oriented system development A system development methodology that is organized around "objects" rather than "actions," and "data" rather than "logic". Scope Note: Object-oriented analysis is an assessment of a physical system to determine which objects in the real world need to be represented as objects in a software system. Any object-oriented design is software design that is centered around designing the objects that will make up a program. Any object-oriented program is one that is composed of objects or software parts.
SPANISH: **Desarrollo de sistemas orientado a objetos (OOSD)**

Offline files Computer file storage media not physically connected to the computer; typically tapes or tape cartridges used for backup purposes.
SPANISH: **Archivos fuera de línea**

Offsite storage A facility located away from the building housing the primary information processing facility (IPF), used for storage of computer media such as offline backup data and storage files.
SPANISH: **Almacenamiento fuera de la sede (offsite)**

Online data processing Achieved by entering information into the computer via a video display terminal. Scope Note: With online data processing, the computer immediately accepts or rejects the information, as it is entered.
SPANISH: **Procesamiento de datos en línea (online)**

Open Source Security Testing Methodology An open and freely available methodology and manual for security testing.
SPANISH: **Metodología de Pruebas de Seguridad de Código Abierto**

Open systems Systems for which detailed specifications of their components composition are published in a nonproprietary environment, thereby enabling competing organizations to use these standard components to build competitive systems. Scope Note: The advantages of using open systems include portability, interoperability and integration.
SPANISH: **Sistema abiertos**

Operating system A master control program that runs the computer and acts as a scheduler and traffic controller. Scope Note: The operating system is the first program copied into the computer's memory after the computer is turned on and must reside in memory at all times. It is the software that interfaces between the computer hardware (disk, keyboard, mouse, network, modem, printer) and the application software (word processor, spreadsheet, e-mail), which also controls access to the devices and is partially responsible for security components and sets the standards for the application programs that run in it.
SPANISH: **Sistema operativo**

Operating system audit trails Records of system events generated by a specialized operating system mechanism.
SPANISH: **Registros de auditoría del sistema operativo**

Operational audit An audit designed to evaluate the various internal controls, economy and efficiency of a function or department.
SPANISH: **Auditoria operativa**

Operational control These controls deal with the everyday operation of a company or organization to ensure all objectives are achieved.
SPANISH: **Control operativo**

Operational level agreement (OLA) An internal agreement covering the delivery of services that support the IT organization in its delivery of services.
SPANISH: **Acuerdo de nivel operativo (OLA)**

Operator console A special terminal used by computer operations personnel to control computer and systems operations functions. Scope Note: Operator console terminals typically provide a high level of computer access and should be properly secured.
SPANISH: **Consola del operador**

Optical character recognition Used to electronically scan and input written information from a source document.
SPANISH: **Reconocimiento óptico de caracteres (OCR)**

Optical scanner An input device that reads characters and images that are printed or painted on a paper form into the computer.
SPANISH: **Scanner óptico**

Organization The manner in which an enterprise is structured; can also mean the entity.
SPANISH: **Organización**

Organization for Economic Cooperation and Development (OECD) An international organization helping governments tackle the economic, social, and governance challenges of a global economy. Scope Note: The OECD groups 30 member countries in a unique forum to discuss, develop, and refine economic and social policies.
SPANISH: **Organización para la Cooperación y el Desarrollo Económico (OCDE)**

Outcome Result
SPANISH: **Resultado**

Outcome measures Represent the consequences of actions previously taken and are often referred to as lag indicators. Scope Note: Outcome measures frequently focus on results at the end of a time period and characterize historical performance. They are also referred to as key goal indicators (KGIs) and are used to indicate whether goals have been met. These can be measured only after the fact and, therefore, are called 'lag indicators.'
SPANISH: **Medidas de resultados**

Output analyzer Checks the accuracy of the results produced by a test run. Scope Note: There are three types of checks that an output analyzer can perform. First, if a standard set of test data and test results exists for a program, the output of a test run after program maintenance can be compared with the set of results that should be produced. Second, as programmers prepare test data and calculate the expected results, these results can be stored on a file and the output analyzer compares the actual results of a test run with the expected results. Third, the output analyzer can act as a query language; it accepts queries about whether certain relationships exist in the file of output results and reports compliance or noncompliance.
SPANISH: **Analizador de salida**

Outsourcing A formal agreement with a third party to perform IS or other business functions for an organization.
SPANISH: **Externalización (outsourcing)**

P

Packet Data unit that is routed from source to destination in a packet-switched network. Scope Note: A packet contains both routing information and data. Transmission Control Protocol/Internet Protocol (TCP/IP) is such a packet-switched network.
SPANISH: **Paquete**

Packet filtering Controlling access to a network by analyzing the attributes of the incoming and outgoing packets and either letting them pass, or denying them, based on a list of rules.
SPANISH: **Filtrado de paquetes**

Packet internet groper (PING) An Internet program (ICMP) used to determine whether a specific IP address is accessible or online. It is a network application that uses UDP to verify reachability of another host on the connected network. Scope Note: It works by sending a packet to the specified address and waiting for a reply. PING is used primarily to troubleshoot Internet connections. In addition, Ping reports how many hops are required to connect two Internet hosts. There are both freeware and shareware Ping utilities available for PCs.
SPANISH: **Rastreador de paquetes en Internet (PING)**

Packet switching The process of transmitting messages in convenient pieces that can be reassembled at the destination.
SPANISH: **Conmutación de paquetes**

Paper test A walk-through of the steps of a regular test, but without actually performing the steps. Scope Note: Usually used in disaster recovery and contingency testing, where team members review and become familiar with the plans and their specific roles and responsibilities.
SPANISH: **Prueba en papel**

Parallel simulation Involves the IS auditor writing a program to replicate those application processes that are critical to an audit opinion and using this program to reprocess application system data. Scope Note: The results produced by parallel simulation are compared with the results generated by the application system and any discrepancies identified.
SPANISH: **Simulación paralela**

Parallel testing The process of feeding test data into two systems, the modified system and an alternative system (possibly the original system) and comparing results to demonstrate the consistency and inconsistency between two versions of the application.
SPANISH: **Pruebas paralelas**

Parity check A general hardware control that helps to detect data errors when data are read from memory or communicated from one computer to another. Scope Note: A 1-bit digit (either 0 or 1) is added to a data item to indicate whether the sum of that data item's bit is odd or even. When the parity bit disagrees with the sum of the other bits, the computer reports an error. The probability of a parity check detecting an error is 50 percent.
SPANISH: **Verificación de paridad**

Partitioned file A file format in which the file is divided into multiple sub files and a directory is established to locate each sub file.
SPANISH: **Archivo particionado**

Passive assault Intruders attempt to learn some characteristic of the data being transmitted. Scope Note: With passive assault, intruders may be able to read the contents of the data so the privacy of the data is violated. Alternatively, although the content of the data itself may remain secure, intruders may read and analyze the plaintext source and destination identifiers attached to a message for routing purposes, or they may examine the lengths and frequency of messages being transmitted.
SPANISH: **Asalto pasivo**

Passive response A response option in intrusion detection in which the system simply reports and records the problem detected, relying on the user to take subsequent action.
SPANISH: **Respuesta pasiva**

Password A protected, generally computer-encrypted string of characters that authenticate a computer user to the computer system.
SPANISH: **Contraseña (password)**

Password cracker A tool that tests the strength of user passwords searching for passwords that are easy to guess by repeatedly trying words from specially crafted dictionaries and often also by generating thousands (and in some cases even millions) of permutations of characters, numbers and symbols.
SPANISH: **Software de rompimiento de contraseñas**

Patch management An area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system, in order to maintain up-to-date software and often to address security risks. Scope Note: Patch management tasks include the following: maintaining current knowledge of available patches; deciding what patches are appropriate for particular systems; ensuring that patches are installed properly; testing systems after installation; and documenting all associated procedures, such as specific configurations required. A number of products are available to automate patch management tasks. Patches are sometimes ineffective and can sometimes cause more problems than they fix. Patch management experts suggest that system administrators take simple steps to avoid problems, such as performing backups and testing patches on non-critical systems prior to installations. Patch management can be viewed as part of change management.
SPANISH: **Gestión de parches**

Payback period The length of time needed to recoup the cost of capital investment. Scope Note: Financial amounts in the payback formula are not discounted. Note that the payback period does not take into account cash flows after the payback period and is therefore not a measure of the profitability of an investment project. The scope of the IRR, NPV and payback period is the useful economic life of the project up to a maximum of five years.
SPANISH: **Período de recuperación de la inversión**

Payment system A financial system that establishes the means for transferring money between suppliers and users of funds, ordinarily by exchanging debits or credits between banks or financial institutions.
SPANISH: **Sistema de pago**

Payroll system An electronic system for processing payroll information and the related electronic (e.g., electronic timekeeping and/or human resources system), human (e.g., payroll clerk), and external party (e.g., bank) interfaces. In a more limited sense, it is the electronic system that performs the processing for generating payroll checks and/or bank direct deposits to employees.
SPANISH: **Sistema de nómina**

Penetration testing A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers.
SPANISH: **Prueba de penetración**

Performance In IT, the actual implementation or achievement of a process.
SPANISH: **Desempeño**

Performance drivers Measures that are considered the "drivers" of lag indicators. They can be measured before the outcome is clear and, therefore, are called "lead indicators." Scope Note: There is an assumed relationship between the two that suggests that improved performance in a leading indicator will drive better performance in the lagging indicator. They are also referred to as key performance indicators (KPIs) and are used to indicate whether goals are likely to be met.
SPANISH: **Factores del desempeño**

Performance indicators A set of metrics designed to measure the extent to which performance objectives are being achieved on an on-going basis. Scope Note: Performance indicators can include service level agreements, critical success factors, customer satisfaction ratings, internal or external benchmarks, industry best practices and international standards.
SPANISH: **Indicadores del desempeño**

Performance management In IT, the ability to manage any type of measurement including employee, team, process, operational or financial measurements. The term connotes closed-loop control and regular monitoring of the measurement.
SPANISH: **Gestión del desempeño**

Performance testing Comparing the system's performance to other equivalent systems using well defined benchmarks.
SPANISH: **Pruebas de rendimiento**

Peripherals Auxiliary computer hardware equipment used for input, output and data storage. Scope Note: Examples of peripherals include disk drives and printers.
SPANISH: **Periféricos**

Personal digital assistant (PDA) Also called palmtop and pocket computer, these are handheld devices that provide computing, Internet, networking and telephone characteristics.
SPANISH: **Asistente digital personal (PDA, Personal Digital Assistant)**

Personal identification number (PIN) A type of password (i.e., a secret number assigned to an individual) that, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual Scope Note: PINs have been adopted by financial institutions as the primary means of verifying customers in an electronic funds transfer system (EFTS).
SPANISH: **Número de identificación personal (PIN)**

Pervasive IS controls General controls which are designed to manage and monitor the IS environment and which, therefore, affect all IS-related activities.
SPANISH: **Controles de SI detallados**

Phase of BCP A step-by-step approach consisting of various phases Scope Note: Phase of BCP is usually comprised of the following phases: pre-implementation phase, implementation phase, testing phase, and post-implementation phase.
SPANISH: **Fase del BCP**

Phishing This is a type of e-mail attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering. Scope Note: Phishing attacks may take the form of masquerading as a lottery organization advising the recipient of a large win or the user's bank; in either case, the intent is to obtain account and PIN details. Alternative attacks may seek to obtain apparently innocuous business information, which may be used in another form of active attack.
SPANISH: **Phishing**

Phreakers Those who crack security, most frequently phone and other communications networks.
SPANISH: **Phreakers**

Piggy backing 1. Following an authorized person into a restricted access area. 2. Electronically attaching to an authorized telecommunications link to intercept and possibly alter transmissions.
SPANISH: **Piggybacking**

Plaintext Digital information, such as cleartext, that is intelligible to the reader.
SPANISH: **Texto plano**

PMBOK Project Management Body of Knowledge (PMBOK), a project management standard developed by the Project Management Institute (PMI).
SPANISH: **PMBOK**

Point-of-presence (POP) A phone number that represents the area in which the communications provider or Internet service provider (ISP) provides service.
SPANISH: **Punto de presencia (POP)**

Point-of-sale (POS) systems Enable the capture of data at the time and place of transaction. Scope Note: POS terminals may include use of optical scanners for use with bar codes or magnetic card readers for use with credit cards. POS systems may be online to a central computer or may use stand-alone terminals or microcomputers that hold the transactions until the end of a specified period when they are sent to the main computer for batch processing.
SPANISH: **Sistemas punto de venta (POS)**

Point-to-point Protocol (PPP) A protocol used for transmitting data between two ends of a connection.
SPANISH: **Protocolo punto a punto (PPP)**

Point-to-point Tunneling Protocol (PPTP) A protocol used to transmit data securely between two end points to create a VPN.
SPANISH: **Protocolo de túnel punto a punto (PPTP)**

Policy Generally, a document that records a high-level principle or course of action which has been decided upon. A policy's intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by the enterprise's management teams. Scope Note: In addition to policy content, policies need to describe the consequences of failing to comply with the policy, the means for handling exceptions, and the manner in which compliance with the policy will be checked and measured
SPANISH: **Política**

Polymorphism (Objects) Polymorphism refers to database structures that send the same command to different child objects that can produce different results depending on their family hierarchical tree structure.
SPANISH: **Polimorfismo (objetos)**

Population The entire set of data from which a sample is selected and about which the IS auditor wishes to draw conclusions.
SPANISH: **Población**

Portfolio A grouping of "objects of interest" (investment programs, IT services, IT projects, other IT assets or resources) managed and monitored to optimize business value. (The investment portfolio is of primary interest to Val IT. IT service, project, asset and other resource portfolios are of primary interest to COBIT).
SPANISH: **Portafolio**

Posting The process of actually entering transactions into computerized or manual files. Scope Note: Posting transactions might immediately update the master files or may result in memo posting, in which the transactions are accumulated over a period of time, then applied to master file updating.
SPANISH: **Enviar (posting)**

Preventive application controls Application controls that are intended to prevent an error from occurring. Preventive application controls are typically executed at the transaction level, before an action is performed.
SPANISH: **Controles preventivos de aplicación**

Preventive control An internal control that is used to avoid undesirable events, errors and other occurrences that an organization has determined could have a negative material effect on a process or end product
SPANISH: **Control preventivo**

PRINCE2 Projects in a Controlled Environment (PRINCE2), developed by the OGC, is a project management method that covers the management, control and organization of a project.
SPANISH: **PRINCE2**

Privacy Freedom from unauthorized intrusion or disclosure of information about individuals.
SPANISH: **Privacidad**

Private branch exchange (PBX) A telephone exchange that is owned by a private business, as opposed to one owned by a common carrier or by a telephone company.
SPANISH: **Centralita (private branch exchange, PBX)/Central telefónica**

Private key A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.
SPANISH: **Clave privada**

Private key cryptosystems Used in data encryption, it uses a secret key to encrypt the plaintext to the ciphertext. Private key cryptosystems also use the same key to decrypt the ciphertext to the corresponding plaintext. Scope Note: In this case, the key is symmetric such that the encryption key is equivalent to the decryption key.
SPANISH: **Criptosistemas de clave privada**

Privilege The level of trust with which a system object is imbued.
SPANISH: **Privilegio**

Problem In IT, the unknown underlying cause of one or more incidents.
SPANISH: **Problema**

Problem escalation procedure The process of escalating a problem up from junior to senior support staff, and ultimately to higher levels of management. Scope Note: Problem escalation procedure is often used in help desk management, where an unresolved problem is escalated up the chain of command, until it is solved.
SPANISH: **Procedimiento de escalacion de problema**

Procedure A document containing steps that specify how to achieve an activity. Procedures are defined as part of processes.
SPANISH: **Procedimiento**

Process Generally, a collection of activities influenced by the enterprise's policies and procedures that takes inputs from a number of sources, (including other processes), manipulates the inputs and produces outputs. Scope Note: Processes have clear business reasons for existing, accountable owners, clear roles and responsibilities around the execution of the process, and the means to measure performance.
SPANISH: **Proceso**

Process maturity assessment A subjective assessment technique derived from the SEI CMMI concepts and developed as a COBIT management tool. It provides management with a profile of how well developed are the IT management processes. Scope Note: It enables management to easily place itself on a scale and appreciate what is required if improved performance is needed. It is used to set targets, raise awareness, capture broad consensus, identify improvements and positively motivate change.
SPANISH: **Evaluación del nivel de madurez de un proceso**

Process maturity attributes The different aspects of a process covered in an assurance initiative.
SPANISH: **Atributos de la madurez del proceso**

Production programs Programs that are used to process live or actual data that were received as input into the production environment.
SPANISH: **Programas de producción**

Production software Software that is being used and executed to support normal and authorized organizational operations. Scope Note: Production software is to be distinguished from test software, which is being developed or modified, but has not yet been authorized for use by management.
SPANISH: **Software de producción**

Professional competence Proven level of ability, often linked to qualifications issued by relevant professional bodies and compliance with their codes of practice and standards.
SPANISH: **Competencia profesional**

Professional standards Refers to standards issued by ISACA. The term mayto related guidelines and techniques that assist the professional in implementing and complying with authoritative pronouncements of ISACA. In certain instances, standards of other professional organizations may be considered, depending on the circumstances and their relevance and appropriateness.
SPANISH: **Normas profesionales**

Program A structured grouping of interdependent projects that is both necessary and sufficient to achieve a desired business outcome and create value. These projects could include, but not be limited to, changes in the nature of the business, business processes, the work performed by people, as well as the competencies required to carry out the work, enabling technology, and organizational structure.
SPANISH: **Programa**

Program Evaluation and Review Technique (PERT) A project management technique used in the planning and control of system projects.
SPANISH: **Técnica de evaluación y revisión del programa (program evaluation and review technique – PERT)**

Program flowcharts Program flowcharts show the sequence of instructions in a single program or subroutine. Scope Note: The symbols used in program flowcharts should be the internationally accepted standard. Program flowcharts should be updated when necessary.
SPANISH: **Diagramas de flujo del programa**

Program narratives Program narratives provide a detailed explanation of program flowcharts, including control points and any external input.
SPANISH: **Narrativas/comentarios de programas**

Project A structured set of activities concerned with delivering a defined capability (that is necessary but not sufficient to achieve a required business outcome) to the enterprise based on an agreed-upon schedule and budget.
SPANISH: **Proyecto**

Project management officer (PMO) The individual function responsible for the implementation of a specified initiative for supporting the project management role and advancing the discipline of project management.
SPANISH: **Oficial de gestión de proyectos (PMO)**

Project portfolio The set of projects owned by a company. Scope Note: It usually includes the main guidelines relative to each project, including objectives, costs, timelines and other information specific to the project.
SPANISH: **Cartera (portfolio) de proyectos**

Project team Group of people responsible for a project, whose terms of reference may include the development, acquisition, implementation or maintenance of an application system. Scope Note: The project team members may include line management, operational line staff, external contractors and IS auditors.
SPANISH: **Equipo del proyecto**

Promiscuous mode Allows the network interface to capture all network traffic irrespective of the hardware device to which the packet is addressed.
SPANISH: **Modo promiscuo**

Protection domain The area of the system that the intrusion detection system is meant to monitor and protect.
SPANISH: **Dominio de protección**

Protocol The rules by which a network operates and controls the flow and priority of transmissions.
SPANISH: **Protocolo**

Protocol converter Hardware devices, such as asynchronous and synchronous transmissions, that convert between two different types of transmission.
SPANISH: **Convertidor de protocolos**

Protocol stack A set of utilities that implement a particular network protocol. Scope Note: For instance, in Windows machines a TCP/IP stack consists of TCP/IP software, sockets software and hardware driver software.
SPANISH: **Pila de protocolo**

Prototyping The process of quickly putting together a working model (a prototype) in order to test various aspects of a design, illustrate ideas or features and gather early user feedback. Scope Note: Prototyping uses programmed simulation techniques to represent a model of the final system to the user for advisement and critique. The emphasis is on end-user screens and reports. Internal controls are not a priority item since this is only a model.
SPANISH: **Prototipado**

Proxy server A server that acts on behalf of a user. Scope Note: Typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps perform additional authentication, and complete a connection to a remote destination on behalf of the user.
SPANISH: **Servidor proxy**

Public key In an asymmetric cryptographic scheme, the key that may be widely published to enable the operation of the scheme.
SPANISH: **Clave pública**

Public key cryptosystem Used in data encryption, it uses an encryption key, as a public key, to encrypt the plaintext to the ciphertext. It uses the different decryption key, as a secret key, to decrypt the ciphertext to the corresponding plaintext. Scope Note: In contrast to a private key cryptosystem, the decryption key should be secret; however, the encryption key can be known to everyone. In a public key cryptosystem, two keys are asymmetric, such that the encryption key is not equivalent to the decryption key.
SPANISH: **Criptosistema de clave pública**

Public key encryption A cryptographic system that uses two keys. One is a public key, which is known to everyone, and the second is a private or secret key, which in only known to the recipient of the message.
SPANISH: **Encriptación de clave pública**

Public key infrastructure (PKI) A series of processes and technologies for the association of cryptographic keys with the entity to whom those keys were issued.
SPANISH: **Infraestructura de clave pública (PKI)**

Q

Quality assurance (QA) A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements. (ISO/IEC 24765)
SPANISH: **Aseguramiento de la calidad (quality assurance)**

Quality management system (QMS) A system that outlines the policies and procedures necessary to improve and control the various processes that will ultimately lead to improved organization performance.
SPANISH: **Sistema de gestión de la calidad (QMS)**

Queue A group of items that is waiting to be serviced or processed.
SPANISH: **Cola**

Quick ship A recovery solution provided by recovery and/or hardware vendors and includes a pre-established contract to deliver hardware resources within a specified number amount of hours after a disaster occurs. Scope Note: The quick ship solution usually provides organizations with the ability to recover within 72 hours or greater.
SPANISH: **Envío rápido**

R

RACI chart Illustrates who is responsible, accountable, consulted and informed within an organizational framework.
SPANISH: **Cuadro de definición de responsabilidades por cargo (RACI)**

Radio wave interference The superposition of two or more radio waves resulting in a different radio wave pattern that is more difficult to intercept and decode properly.
SPANISH: **Interferencia de onda de radio**

Random access memory (RAM) The computer's primary working memory. Scope Note: Each byte of random access memory can be accessed randomly regardless of adjacent bytes.
SPANISH: **Memoria de acceso aleatorio (RAM)**

Range check Range checks ensure that data fall within a predetermined range.
SPANISH: **Verificación del rango**

Rapid application development A methodology that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality by using a series of proven application development techniques, within a well-defined methodology.
SPANISH: **Desarrollo rápido de aplicaciones**

Real-time analysis Analysis that is performed on a continuous basis, with results gained in time to alter the run-time system.
SPANISH: **Análisis en tiempo real**

Real-time processing An interactive online system capability that immediately updates computer files when transactions are initiated through a terminal.
SPANISH: **Procesamiento en tiempo real**

Reasonable assurance A level of comfort short of a guarantee but considered adequate given the costs of the control and the likely benefits achieved.
SPANISH: **Aseguramiento razonable**

Reasonableness check Compares data to predefined reasonability limits or occurrence rates established for the data.
SPANISH: **Comprobación de razonabilidad**

Reciprocal agreement Emergency processing agreements between two or more organizations with similar equipment or applications. Scope Note: Typically, participants of a reciprocal agreement promise to provide processing time to each other when an emergency arises.
SPANISH: **Acuerdo recíproco**

Record A collection of related information treated as a unit. Scope Note: Separate fields within the record are used for processing of the information.
SPANISH: **Registro**

Record, screen and report layouts Record layouts provide information regarding the type of record, its size and the type of data contained in the record. Screen and report layouts describe what information is provided and necessary for input.
SPANISH: **Diseños de registros, pantallas e informes**

Recovery action Execution of a response or task according to a written procedure.
SPANISH: **Acción de recuperación**

Recovery point objective (RPO) The RPO is determined based on the acceptable data loss in case of a disruption of operations. It indicates the earliest point in time to which it is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption.
SPANISH: **Objetivo de punto de recuperación (RPO)**

Recovery strategy An approach by an organization that will ensure its recovery and continuity in the face of a disaster or other major outage. Scope Note: Plans and methodologies are determined by the organization's strategy. There may be more than one methodology or solution for an organization's strategy. Examples of methodologies and solutions include: contracting for hot site or cold site, building an internal hot site or cold site, identifying an alternate work area, a consortium or reciprocal agreement, contracting for mobile recovery or crate and ship, and many others.
SPANISH: **Estrategia de recuperación**

Recovery testing A test to check the system's ability to recover after a software or hardware failure.
SPANISH: **Pruebas de recuperación**

Recovery time objective (RTO) The amount of time allowed for the recovery of a business function or resource after a disaster occurs
SPANISH: **Objetivo de tiempo de recuperación (RTO)**

Redo logs Files maintained by a system, primarily a database management system, for the purposed of reapplying changes following an error or outage recovery.
SPANISH: **Logs de Recuperación de registros u operaciones ante fallas**

Redundancy check Detects transmission errors by appending calculated bits onto the end of each segment of data.
SPANISH: **Verificación de redundancia**

Redundant Array of Inexpensive Disks (RAID) Provides performance improvements and fault-tolerant capabilities via hardware or software solutions, by writing to a series of multiple disks to improve performance and/or save large files simultaneously.
SPANISH: **Conjunto redundante de discos de bajo costo (RAID)**

Redundant site A recovery strategy involving the duplication of key information technology components, including data or other key business processes, whereby fast recovery can take place.
SPANISH: **Sitio redundante**

Reengineering A process involving the extraction of components from existing systems and restructuring these components to develop new systems or to enhance the efficiency of existing systems. Scope Note: Existing software systems can be modernized to prolong their functionality. An example of this is a software code translator that can take an existing hierarchical database system and transpose it to a relational database system. CASE includes a source code reengineering feature.
SPANISH: **Reingeniería**

Registration authority (RA) The individual of institution that validates and entity's proof of identity and ownership of a key pair.
SPANISH: **Autoridad de registro (RA)**

Regression testing A testing technique used to retest earlier program abends or logical errors that occurred during the initial testing phase.
SPANISH: **Pruebas de regresión**

Relational database management system (RDBMS) The general purpose of a database is to store and retrieve related information. Scope Note: Database management systems have evolved from hierarchal to network to relational models. Today, the most widely accepted database model is the relational model. The relational model has three major aspects, structures, operations and integrity rules. An Oracle database is a collection of data that is treated as a unit.
SPANISH: **Sistema de administración de bases de datos relacionales (RDBMS)**

Relevant audit evidence Audit evidence is relevant if it pertains to the audit objectives and has a logical relationship to the findings and conclusions it is used to support.
SPANISH: **Evidencia de auditoría relevante**

Reliable audit evidence Audit evidence is reliable if, in the IS auditor's opinion, it is valid, factual, objective and supportable.
SPANISH: **Evidencia de auditoría confiable**

Remote access service (RAS) Refers to any combination of hardware and software to enable the remote access to tools or information that typically reside on a network of IT devices. Scope Note: Originally coined by Microsoft when referring to their built-in NT remote access tools, RAS was a service provided by Windows NT which allows most of the services that which would be available on a network to be accessed over a modem link. Over the years, many vendors have provided both hardware and software solutions to gain remote access to various types of networked information. In fact, most modern routers include a basic RAS capability that can be enabled for any dial-up interface.
SPANISH: **Servicio de acceso remoto (remote access service, RAS)**

Remote Authentication Dial-in User Service (RADIUS) A type of service providing an authentication and accounting system often used for dial-up and remote access security.
SPANISH: **Servicio de autenticación remota telefónica de usuario (RADIUS)**

Remote job entry (RJE) The transmission of job control language (JCL) and batches of transactions from a remote terminal location.
SPANISH: **Entrada remota de trabajos (RJE)**

Remote procedure call (RPC) The traditional Internet service protocol widely used for many years on UNIX-based operating systems and supported by the Internet Engineering Task Force (IETF) that allows a program on one computer to execute a program on another (e.g., server). Scope Note: The primary benefit derived from its use is that a system developer need not develop specific procedures for the targeted computer system. For example, in a client-server arrangement, the client program sends a message to the server with appropriate arguments, and the server returns a message containing the results of the program executed. Common Object Request Broker Architecture (CORBA) and Distributed Component Object Model (DCOM) are two newer object-oriented methods for related RPC functionality.
SPANISH: **Llamada a procedimiento remoto (RPC)**

Repeaters A physical layer device that regenerates and propagates electrical signals between two network segments. Scope Note: Repeaters receive signals from one network segment and amplify (regenerate) the signal to compensate for signals (analog or digital) distorted by transmission loss due to reduction of signal strength during transmission (i.e., attenuation)
SPANISH: **Repetidores**

Replication In its broad computing sense, involves the use of redundant software or hardware elements to provide availability and fault-tolerant capabilities. In a database context, replication involves the sharing of data between databases to reduce workload among database servers, thereby improving client performance, while maintaining consistency among all systems.
SPANISH: **Replicación**

Repository An enterprise database that stores and organizes data.
SPANISH: **Repositorio**

Repudiation The denial by one of the parties to a transaction, or participation in all or part of that transaction, or of the content of communications related to that transaction
SPANISH: **Repudio**

Reputation risk The current and prospective effect on earnings and capital arising from negative public opinion. Scope Note: Reputation risk affects the bank's ability to establish new relationships or services, or continue servicing existing relationships. It may expose the bank to litigation, financial loss or a decline in its customer base. A bank's reputation can be damaged by Internet banking services that are executed poorly or otherwise alienate customers and the public. An Internet bank has a greater reputation risk, as compared to a traditional brick-and-mortar bank, since it is easier for its customers to leave and go to a different Internet bank and since it cannot discuss any problems with the customer in person.
SPANISH: **Riesgo de la reputación**

Request for comments (RFC) A document that has been approved by the IETF becomes an RFC and is assigned a unique number once published. Scope Note: If RFC gains enough interest, it may evolve into an Internet standard.
SPANISH: **Solicitud de comentarios (RFC)**

Request for proposal (RFP) A document distributed to software vendors requesting them to submit a proposal to develop or provide a software product.
SPANISH: **Petición de propuestas (RFP)**

Requirements definition A technique used where the affected user groups define the requirements of the system for meeting the defined needs. Scope Note: Some of these requirements are business, regulatory, security as well as development related.
SPANISH: **Definición de requerimientos**

Residual risk The remaining risk after management has implemented risk response
SPANISH: **Riesgo residual**

Resilience The ability of a system or network to resist failure or to recover quickly from any disruption, usually with minimal recognizable effect
SPANISH: **Tolerancia a falla**

Responsible In a RACI chart, refers to the person who must ensure that activities are completed successfully.
SPANISH: **Responsable**

Return on investment (ROI) A measure of operating performance and efficiency, computed in its simplest form by dividing net income by the total investment over the period being considered.
SPANISH: **Retorno de la inversión (ROI)**

Reverse engineering A software engineering technique whereby an existing application system code can be redesigned and coded using computer-aided software engineering (CASE) technology.
SPANISH: **Ingeniería inversa/reversa**

Ring configuration Used in either token ring or FDDI networks, all stations (nodes) are connected to a multi-station access unit (MSAU), which physically resembles a star-type topology. Scope Note: A ring configuration is created when these MSAUs are linked together in forming a network. Messages in this network are sent in a deterministic fashion from sender and receiver via a small frame, referred to as a token ring. To send a message, a sender obtains the token with the right priority as the token travels around the ring, with receiving nodes reading those messages addressed to it.
SPANISH: **Configuración de anillo**

Ring topology A type of LAN architecture in which the cable forms a loop, with stations attached at intervals around the loop. Scope Note: In ring topology, signals transmitted around the ring take the form of messages. Each station receives the messages and each station determines, on the basis of an address, whether to accept or process a given message. However, after receiving a message, each station acts as a repeater, retransmitting the message at its original signal strength
SPANISH: **Topología de anillo**

Risk The combination of the probability of an event and its consequence. (ISO/IEC73)
SPANISH: **Riesgo**

Risk aggregation The process of integrating risk assessments at a corporate level to obtain a complete view on the overall risk for the enterprise
SPANISH: **Consolidación de riesgos**

Risk analysis 1. A process by which frequency and magnitude of IT risk scenarios are estimated 2. The initial steps of risk management: analyzing the value of assets to the business, identifying threats to those assets and evaluating how vulnerable each asset is to those threats Scope Note: It often involves an evaluation of the probable frequency of a particular event, as well as the probable impact of that event.
SPANISH: **Análisis de riesgos**

Risk appetite The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission
SPANISH: **Apetito al riesgo**

Risk assessment A process used to identify and evaluate risks and their potential effects. Scope Note: Risk assessment includes assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.
SPANISH: **Evaluación de riesgo**

Risk avoidance The process for systematically avoiding risk, constituting one approach to managing risk.
SPANISH: **Evitar los riesgos**

Risk culture The set of shared values and beliefs that governs attitudes toward risk-taking, care and integrity, and determines how openly risks and losses are reported and discussed
SPANISH: **Cultura de riesgos**

Risk evaluation The process of comparing the estimated risk against given risk criteria to determine the significance of the risk. [ISO/IEC Guide 73:2002]
SPANISH: **Evaluación del riesgo**

Risk factor A condition that can influence the frequency and/or magnitude and, ultimately, the business impact of IT-related events/scenarios
SPANISH: **Factor de riesgo**

Risk indicator A metric capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite
SPANISH: **Indicador de riesgo**

Risk management The coordinated activities to direct and control an organization with regard to risk.

(In the International Standard, the term "control" is used as a synonym for "measure" ISO/IEC Guide 73:2002).
SPANISH: **Gestión de riesgos**

Risk map A (graphic) tool for ranking and displaying risks by defined ranges for frequency and magnitude
SPANISH: **Mapa de riesgos**

Risk mitigation The management of risk through the use of countermeasures and controls.
SPANISH: **Mitigación del riesgo**

Risk portfolio view 1. A method to identify interdependencies and interconnections among risks, as well as the effect of risk responses on multiple risks 2. A method to estimate the aggregate impact of multiple risks (e.g., cascading and coincidental threat types/scenarios, risk concentration/correlation across silos) and the potential effect of risk response across multiple risks
SPANISH: **Vista de la cartera de riesgos**

Risk tolerance The acceptable level of variation that management is willing to allow for any particular risk as it pursues objectives
SPANISH: **Tolerancia al riesgo**

Risk transfer The process of assigning risk to another organization, usually through the purchase of an insurance policy or outsourcing the service.
SPANISH: **Transferencia del riesgo**

Risk treatment The process of selection and implementation of measures to modify risk [ISO/IEC Guide 73:2002].
SPANISH: **Tratamiento de riesgos**

Root cause analysis Process of diagnosis to establish origins of events, which can be used for learning from consequences, typically of errors and problems.
SPANISH: **Análisis de causa raíz**

Rootkit A software suite designed to aid an intruder in gaining unauthorized administrative access to a computer system.
SPANISH: **Rootkit**

Rotating standby A fail-over process in which there are two nodes (as in idle standby but without priority). Scope Note: The node that enters the cluster first owns the resource group, and the second will join as a standby node.
SPANISH: **Modo en espera rotativo**

Rounding down A method of computer fraud involving a computer code that instructs the computer to remove small amounts of money from an authorized computer transaction by rounding down to the nearest whole value denomination and rerouting the rounded off amount to the perpetrator's account.
SPANISH: **Redondear hacia abajo**

Router A networking device that can send (route) data packets from one local area network (LAN) or wide area network (WAN) to another, based on addressing at the network layer (Layer 3) in the OSI model. Scope Note: Networks connected by routers can use different or similar networking protocols. Routers usually are capable of filtering packets based on parameters, such as source addresses, destination addresses, protocol and network applications (ports).
SPANISH: **Enrutador (router)**

RS-232 interface Interface between data terminal equipment and data communications equipment employing serial binary data interchange.
SPANISH: **Interfaz RS-232**

RSA A public key cryptosystem developed by R. Rivest, A. Shamir and L. Adleman used for both encryption and digital signatures. Scope Note: The RSA has two different keys, the public encryption key and the secret decryption key. The strength of the RSA depends on the difficulty of the prime number factorization. For applications with high-level security, the number of the decryption key bits should be greater than 512 bits.
SPANISH: **RSA**

Rulebase The list of rules and/or guidance that is used to analyze event data.
SPANISH: **Reglas básicas**

Run instructions Computer operating instructions which detail the step-by-step processes that are to occur so an application system can be properly executed; also identifies how to address problems that occur during processing.
SPANISH: **Instrucciones de ejecución**

Run-to-run totals Provide evidence that a program processes all input data and that it processed the data correctly.
SPANISH: **Totales de ejecución en ejecucion (run-torun totals)**

S

Safeguard A practice, procedure or mechanism that reduces risk.
SPANISH: **Protección**

Salami technique A method of computer fraud involving a computer code that instructs the computer to slice off small amounts of money from an authorized computer transaction and reroute this amount to the perpetrator's account.
SPANISH: **Técnica del salami**

Sampling risk The probability that the IS auditor has reached an incorrect conclusion because an audit sample, rather than the whole population, was tested Scope Note: While sampling risk can be reduced to an acceptably low level by using an appropriate sample size and selection method, it can never be eliminated.
SPANISH: **Riesgo de muestreo**

Scheduling A method used in the information processing facility (IPF) to determine and establish the sequence of computer job processing.
SPANISH: **Planificación (scheduling)**

Scope creep Also called requirement creep, this refers to uncontrolled changes in a project's scope. Scope Note: Scope creep can occur when the scope of a project is not properly defined, documented and controlled. Typically, the scope increase consists of either new products or new features of already approved products. Hence, the project team drifts away from its original purpose. Because of one's tendency to focus on only one dimension of a project, scope creep can also result in a project team overrunning its original budget and schedule. For example, scope creep can be a result of poor change control, lack of proper identification of what products and features are required to bring about the achievement of project objectives in the first place, or a weak project manager or executive sponsor.
SPANISH: **Desviación del alcance (scope creep)**

Scoping process Identifying the boundary or extent to which a process, procedure, certification, contract, etc., applies.
SPANISH: **Proceso de identificación del alcance**

Screening routers A router configured to permit or deny traffic based on a set of permission rules installed by the administrator.
SPANISH: **Enrutadores de filtrado (screening routers)**

Secure Sockets Layer (SSL) A protocol that is used to transmit private documents through the Internet. Scope Note: The SSL protocol uses a private key to encrypt the data that is to be transferred through the SSL connection.
SPANISH: **Capa de conector seguro (SSL)**

Security administrator The person responsible for implementing, monitoring and enforcing security rules established and authorized by management.
SPANISH: **Administrador de seguridad**

Security awareness The extent to which every member of an organization and every other individual who potentially has access to the organization's information
understand:
Security and the levels of security appropriate to the organization
The importance of security and consequences of a lack of security
Their individual responsibilities regarding security (and act accordingly). Scope Note: This definition is based on the definition for IT security awareness as defined in Implementation Guide: How to Make Your Organization Aware of IT Security, European Security(ESF), London, UK, 1993)
SPANISH: **Concienciación de la seguridad**

Security awareness campaign A predefined, organized number of actions aimed at improving the security awareness of a special target audience about a specific security problem. Each security awareness program consists of a number of security awareness campaigns.
SPANISH: **Campaña de concienciación de la seguridad**

Security awareness coordinator Individual responsible for setting up and maintaining the security awareness program and coordinating the different campaigns and efforts of the various groups involved in the program. He/she is also responsible for making sure all materials are prepared, advocates/trainers are trained, campaigns are scheduled, events are publicized and the program as a whole moves forward.
SPANISH: **Coordinador de concienciación de la seguridad**

Security awareness program A clearly and formally defined plan, structured approach, and set of related activities and procedures with the objective of realizing and maintaining a security- aware culture. Scope Note: This definition clearly states that it is about realizing and maintaining a security-aware culture, meaning attaining and sustaining security awareness at all times. This implies that a security awareness program is not a one-time effort but a continuous process.
SPANISH: **Programa de concienciación de la seguridad**

Security forum Responsible for information security governance within the organization. Scope Note: A security forum can be part of an existing management body. As information security is a business responsibility shared by all members of the executive management team, the forum needs to involve executives from all significant parts of the organization. Typically, a security forum has the following tasks and responsibilities:
Defining a security strategy in line with the business strategy
Identifying security requirements
Establishing a security policy
Drawing up an overall security program or plan
Approving major initiatives to enhance information security
Reviewing and monitoring information security incidents
Monitoring significant changes in the exposure of information assets to major threats
SPANISH: **Foro de seguridad**

Security incident A series of unexpected events that involves an attack or series of attacks (compromise and/or breach of security) at one or more sites. A security incident normally includes an estimation of its level of impact. A limited number of impact levels are defined and, for each, the specific actions required and the people who need to be notified are identified
SPANISH: **Incidente de seguridad**

Security management The process of establishing and maintaining security in a computer or network system. Scope Note: The stages of the process of security management include prevention of security problems, detection of intrusions, investigation of intrusions and resolution. In network management, controlling access to the network and resources, finding intrusions, identifying entry points for intruders and repairing or otherwise closing those avenues of access.
SPANISH: **Gestión de la seguridad**

Security metrics A standard of measurement used in management of security related activities.
SPANISH: **Métricas de seguridad**

Security perimeter The boundary that defines the area of security concern and security policy coverage.
SPANISH: **Perímetro de seguridad**

Security policy A high-level document representing an organization'ssecurity philosophy and commitment.
SPANISH: **Política de seguridad**

Security procedures The formal documentation of specific operational steps and processes that specify how security goals and objectives set forward in the security policy and standards are to be achieved.
SPANISH: **Procedimientos de seguridad**

Security software Software used to administer security, which usually includes authentication of users, access granting according to predefined rules, monitoring and reporting functions.
SPANISH: **Software de seguridad**

Security standards Practices, directives, guidelines, principles or baselines that state what needs to be done and focus on areas of current relevance and concern. They are a translation of issues already mentioned in the security policy.
SPANISH: **Normas de seguridad**

Security testing Ensuring the modified or new system includes appropriate controls and does not introduce any security holes that might compromise other systems or misuses of the system or its information.
SPANISH: **Pruebas de seguridad**

Security/transaction risk The current and prospective risk to earnings and capital arising from fraud, error and the inability to deliver products or services, maintain a competitive position, and manage information. Scope Note: Security risk is evident in each product and service offered, and it encompasses product development and delivery, transaction processing, systems development, computing systems, complexity of products and services and the internal control environment. A high level of security risk may exist with Internet banking products, particularly if those lines of business are not adequately planned, implemented and monitored.
SPANISH: **Riesgo de seguridad/transacción**

Segregation/separation of duties A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals responsibility for initiating and recording transactions and custody of assets to separate individuals. Scope Note: Segregation and separation of duties is commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.
SPANISH: **Segregación de funciones**

Sensitivity A measure of the impact that improper disclosure of information may have on an organization.
SPANISH: **Sensibilidad**

Sequence check A verification that the control number follows sequentially and any control numbers out of sequence are rejected or noted on an exception report for further research. Scope Note: Can be alpha or numeric and usually utilizes a key field.
SPANISH: **Verificación de secuencias**

Sequential file A computer file storage format in which one record follows another. Scope Note: Records can be accessed sequentially only. It is required with magnetic tape.
SPANISH: **Archivo secuencial**

Service bureau A computer facility that provides data processing services to clients on a continual basis.
SPANISH: **Servicio externo (service bureau)**

Service delivery objective (SDO) Directly related to the business needs, SDO is the level of services to be reached during the alternate process mode until the normal situation is restored.
SPANISH: **Objetivos de entrega del servicio (SDO)**

Service desk The point of contact within the IT organization for users of IT services.
SPANISH: **Centro de servicios**

Service level agreement (SLA) An agreement, preferably documented, between a service provider and the customer(s)/user(s) that defines minimum performance targets for a service and how they will be measured.
SPANISH: **Acuerdo de nivel de servicio (SLA)**

Service provider An organization supplying services to one or more (internal or external) customers.
SPANISH: **Proveedor de servicios**

Service Set Identifier (SSID) A 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. Scope Note: The SSID differentiates one WLAN from another so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plaintext from a packet, it does not supply any security to the network. An SSID is also referred to as a network name, because essentially it is a name that identifies a wireless network.
SPANISH: **Identificador del conjunto de servicios (SSID)**

Service user The organization using the outsourced service.
SPANISH: **Usuario de servicios**

Service-oriented architecture (SOA) A cloud-based library of proven, functional software applets that are able to be connected together to become a useful online application
SPANISH: **Arquitectura orientada a servicios (SOA)**

Servlet A Java applet or a small program that runs within a web server environment. Scope Note: A Java servlet is similar to a CGI program, but unlike a CGI program, once started, it stays in memory and can fulfill multiple requests, thereby saving server execution time and speeding up the services.
SPANISH: **Servlet**

Session border controller (SBC) Provide security features for VoIP traffic similar to that provided by firewalls. Scope Note: SBCs can be configured to filter specific VoIP protocols, monitor for denial-of-service (DOS) attacks, and provide network address and protocol translation features.
SPANISH: **Controladora de límite de sesión (SBC)**

Shell The interface between the user and the system.
SPANISH: **Shell**

Shell programming A script written for the shell, or command line interpreter, of an operating system. It is often considered a simple domain-specific programming language. Scope Note: Typical operations performed by shell scripts include file manipulation, program execution and printing text. Usually, shell script refers to scripts written for a Unix shell, while COMMAND.COM (DOS) and cmd.exe (Windows) command line scripts are usually called batch files. Many shell script interpreters double as command line interface such as the various Unix shells, Windows PowerShell or the MS-DOS COMMAND.COM. Others, such as AppleScript, add scripting capability to computing environments lacking a command line interface. Other examples of programming languages primarily intended for shell scripting include digital command language (DCL) and job control language (JCL).
SPANISH: **Programación en shell**

Sign-on procedure The procedure performed by a user to gain access to an application or operating system. Scope Note: If the user is properly identified and authenticated by the system's security, they will be able to access the software.
SPANISH: **Procedimiento de inicio de sesión**

Simple fail-over A fail-over process in which the primary node owns the resource group. Scope Note: The backup node runs a non-critical application (e.g., a development or test environment) and takes over the critical resource group but not vice versa.
SPANISH: **Tolerancia a fallas simple**

Simple Mail Transport Protocol (SMTP) The standard e-mail protocol on the Internet.
SPANISH: **Protocolo simple de Transporte de Correos (SMTP)**

Simple Object Access Protocol (SOAP) A platform-independent XML-based formatted protocol enabling applications to communicate with each other over the Internet. Scope Note: Use of SOAP may provide a significant security risk to web application operations, since use of SOAP piggybacks onto a web-based document object model and is transmitted via HTTP (port 80) to penetrate server firewalls, which are usually configured to accept port 80 and port 21 (FTP) requests. Web-based document models define how objects on a web page are associated with each other and how they can be manipulated while being sent from a server to a client browser. SOAP typically relies on XML for presentation formatting and also adds appropriate HTTP-based headers to send it. SOAP forms the foundation layer of the Web services stack, providing a basic messaging framework on which more abstract layers can build. There are several different types of messaging patterns in SOAP, but by far the most common is the Remote Procedure Call (RPC) pattern, in which one network node (the client) sends a request message to another node (the server), and the server immediately sends a response message to the client.
SPANISH: **Protocolo simple de acceso a objetos (SOAP)**

Single point of failure A resource whose loss will result in the loss of service or production.
SPANISH: **Punto de falla único**

Slack time (float) Time in the project schedule, the use of which does not affect the project's critical path; the minimum time to complete the project based upon the estimated time for each project segment and their relationships. Scope Note: Slack time is commonly referred to as "float" and generally is not "owned" by either party to the transaction.
SPANISH: **Tiempo de holgura (slack time)**

SMARRT Specific, measurable, actionable, realistic, results-oriented and timely, generally used to describe appropriately set goals.
SPANISH: **SMARRT (Specific, measurable, actionable, realistic, results-oriented and timely)**

Smart card A small electronic device that contains electronic memory, and possibly an embedded integrated circuit. Scope Note: Smart cards can be used for a number of purposes including the storage of digital certificates or digital cash, or it can be used as a token to authenticate users.
SPANISH: **Tarjeta inteligente**

Sniff The act of capturing network packets, including those not necessarily destined for the computer running the sniffing software.
SPANISH: **Captura de paquetes a través de la escucha de la red (Sniff)**

Sniffing The process by which data traversing a network are captured or monitored.
SPANISH: **Búsqueda (sniffing)**

Social engineering An attack based on deceiving users or administrators at the target site into revealing confidential or sensitive information.
SPANISH: **Ingeniería social**

Software Programs and supporting documentation that enable and facilitate use of the computer. Scope Note: Software controls the operation of the hardware and the processing of data.
SPANISH: **Software**

Source code The language in which a program is written. Scope Note: Source code is translated into object code by assemblers and compilers. In some cases, source code may be converted automatically into another language by a conversion program. Source code is not executable by the computer directly. It must first be converted into a machine language.
SPANISH: **Código fuente**

Source code compare programs Provide assurance that the software being audited is the correct version of the software, by providing a meaningful listing of any discrepancies between the two versions of the program.
SPANISH: **Programas de comparación de código fuente**

Source documents The forms used to record data that have been captured. Scope Note: A source document may be a piece of paper, a turnaround document or an image displayed for online data input.
SPANISH: **Documentos fuente**

Source lines of code (SLOC) Often used in deriving single-point software-size estimations.
SPANISH: **Líneas de código fuente (SLOC)**

Spanning port A port configured on a network switch to receive copies of traffic from one or more other ports on the switch
SPANISH: **Puerto de expansión**

Split data systems A condition in which each of an organization's regional locations maintains its own financial and operational data while sharing processing with an organization wide, centralized database. Scope Note: Split data systems permit easy sharing of data while maintaining a certain level of autonomy.
SPANISH: **Sistema de segregación de datos**

Split DNS An implementation of DNS intended to secure responses provided by the server such that different responses are given to internal vs. external users.
SPANISH: **DNS divididos**

Split knowledge A security technique in which two or more entities separately hold data items that individually convey no knowledge of the information that results from combining the items; a condition under which two or more entities separately have key components that individually convey no knowledge of the plain text key that will be produced when the key components are combined in the cryptographic module.
SPANISH: **Conocimiento dividido**

Spoofing Faking the sending address of a transmission in order to gain illegal entry into a secure system.
SPANISH: **Spoofing**

SPOOL (simultaneous peripheral operations online) An automated function that can be operating system or application based in which electronic data being transmitted between storage areas are spooled or stored until the receiving device or storage area is prepared and able to receive the information. Scope Note: Spool allows more efficient electronic data transfers from one device to another by permitting higher speed sending functions, such as internal memory, to continue on with other operations instead of waiting on the slower speed receiving device, such as a printer.
SPANISH: **SPOOL (operaciones periféricas simultáneas en línea)**

Spyware Software whose purpose is to monitor a computer user's actions (e.g., web sites they visit) and report these actions to a third party, without the informed consent of that machine's owner or legitimate user. Scope Note: A particularly malicious form of spyware is software that monitors keystrokes (e.g., to obtain passwords) or otherwise gathers sensitive information such as credit card numbers, which it then transmits to a malicious third party. The term has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.
SPANISH: **Software espía (spyware)**

Stage-gate A point in time when a program is reviewed, and a decision is made to commit expenditures to the next set of activities on a program or project, to stop the work altogether, or to put a hold on execution of further work.
SPANISH: **Etapa-puerta**

Standard A mandatory requirement, code of practice or specification approved by a recognized external standards organization, such as ISO.
SPANISH: **Estándar**

Standing data Permanent reference data used in transaction processing. Scope Note: These data are changed infrequently, such as a product price file or a name and address file.
SPANISH: **Datos permanentes**

Star topology A type of LAN architecture that utilizes a central controller to which all nodes are directly connected. Scope Note: With star topology, all transmissions from one station to another pass through the central controller, which is responsible for managing and controlling all communication. The central controller often acts as a switching device.
SPANISH: **Topología de estrella**

Static analysis Analysis of information that occurs on a non-continuous basis; also known as interval-based analysis.
SPANISH: **Análisis estático**

Statistical sampling A method of selecting a portion of a population, by means of mathematical calculations and probabilities, for the purpose of making scientifically and mathematically sound inferences regarding the characteristics of the entire population.
SPANISH: **Muestreo estadístico**

Storage area networks (SANs) A variation of a LAN that is dedicated for the express purpose of connecting storage devices to servers and other computing devices. Scope Note: SANs centralize the process for the storage and administration of data.
SPANISH: **Redes de área de almacenamiento (SANs)**

Strategic planning The process of deciding on the organization's objectives, on changes in these objectives, and the policies to govern their acquisition and use.
SPANISH: **Planificación estratégica**

Strengths, weaknesses, opportunities and threats (SWOT) A combination of an organizational audit listing the organization's strengths and weaknesses and an environmental scan or analysis of external opportunities and threats.
SPANISH: **Fortalezas, Oportunidades, Debilidades, Amenazas (FODA)**

Structured programming A top-down technique of designing programs and systems that makes programs more readable, more reliable and more easily maintained.
SPANISH: **Programación estructurada**

Structured Query Language (SQL) The primary language used by both application programmers and end users in accessing relational databases.
SPANISH: **Lenguaje de consultas estructuradas (SQL)**

Subject matter The specific information subject to the IS auditor's report and related procedures which can include things such as the design or operation of internal controls and compliance with privacy practices or standards or specified laws and regulations (Area of activity).
SPANISH: **Tema**

Substantive testing Obtaining audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period.
SPANISH: **Pruebas sustantivas**

Sufficient audit evidence Audit evidence is sufficient if it is adequate, convincing and would lead another IS auditor to form the same conclusions.
SPANISH: **Evidencia de auditoría suficiente**

Supply chain management (SCM) A concept that allows an organization to more effectively and efficiently manage the activities of design, manufacturing, distribution, service and recycling of products and services its customers.
SPANISH: **Administración de la cadena de suministro (SCM)**

Surge suppressor Filters out electrical surges and spikes.
SPANISH: **Supresor de picos**

Suspense file A computer file used to maintain information (i.e., on transactions, payments or other events) until the proper disposition of that information can be determined. Scope Note: Once the proper disposition of the item is determined, it should be removed from the suspense file and processed in accordance with the proper procedures for that particular transaction. Two examples of items that may be included in a suspense file are receipt of a payment from a source that is not readily identified or data that do not yet have an identified match during migration to a new application.
SPANISH: **Archivo en suspenso**

Switches Typically associated as a data link layer device, switches enable LAN network segments to be created and interconnected, which also has the added benefit of reducing collision domains in Ethernet-based networks.
SPANISH: **Switches**

Symmetric key encryption System in which a different key (or set of keys) is used by each pair of trading partners to ensure that no one else can read their messages. The same key is used for encryption and decryption. See private key cryptosystem.
SPANISH: **Encriptación por clave simétrica**

Synchronize (SYN) A flag set in the initial setup packets to indicate that the communicating parties are synchronizing the sequence numbers used for the data transmission.
SPANISH: **Sincronizar (SYN)**

Synchronous transmission Block-at-a-time data transmission.
SPANISH: **Transmisión síncrona**

System development life cycle (SDLC) The phases deployed in the development or acquisition of a software system Scope Note: An approach used to plan, design, develop, test and implement an application system or a major modification to an application system. phases of SDLC include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and post-implementation review, but not the service delivery or benefits realization activities.
SPANISH: **Ciclo de Vida del Desarrollo de Sistemas (SDLC)**

System exit Special system software features and utilities that allow the user to perform complex system maintenance. Scope Note: Use of system exits often permits the user to operate outside of the security access control system.
SPANISH: **Salida del sistema**

System flowcharts Graphical representations of the sequence of operations in an information system or program. Scope Note: Information system flowcharts show how data from source documents flow through the computer to final distribution to users. Symbols used should be the internationally accepted standard. System flowcharts should be updated when necessary.
SPANISH: **Diagramas de flujo del sistema**

System narratives Provide an overview explanation of system flowcharts, with explanation of key control points and system interfaces.
SPANISH: **Narrativas del sistema**

System software A collection of computer programs used in the design, processing and control of all applications. Scope Note: The programs and processing routines that control the computer hardware, including the operating system and utility programs.
SPANISH: **Software del sistema**

System testing Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. Scope Note: System test procedures typically are performed by the system maintenance staff in their development library.
SPANISH: **Pruebas del sistema**

Systems acquisition process Procedures established to purchase application software, or an upgrade, including evaluation of the supplier's financial stability, track record, resources and references from existing customers.
SPANISH: **Proceso de adquisición de sistemas**

Systems analysis The systems development phase in which systems specifications and conceptual designs are developed, based on end-user needs and requirements.
SPANISH: **Análisis de sistemas**

T

Table look-ups Used to ensure that input data agree with predetermined criteria stored in a table.
SPANISH: **Búsquedas en tabla**

Tape management system (TMS) A system software tool that logs, monitors and directs computer tape usage.
SPANISH: **Sistema de administración de cintas (TMS)**

Taps Wiring devices that may be inserted into communication links for use with analysis probes, LAN analyzers and intrusion detection security systems.
SPANISH: **Tomas**

Tcpdump A network monitoring and data acquisition tool that performs filter translation, packet acquisition and packet display.
SPANISH: **Tcpdump**

Technical infrastructure security Refers to the security of the infrastructure that supports the ERP networking and telecommunications, operating systems and databases.
SPANISH: **Seguridad de infraestructura técnica**

Technology infrastructure Technology, human resources and facilities that enable the processing and use of applications.
SPANISH: **Infraestructura de tecnología**

Technology infrastructure plan A plan for the technology, human resources and facilities that enable the current and future processing and use of applications.
SPANISH: **Plan de infraestructura de tecnología**

Telecommunications Electronic communications by special devices over distances or around devices that preclude direct interpersonal exchange.
SPANISH: **Telecomunicaciones**

Teleprocessing Using telecommunications facilities for handling and processing of computerized information.
SPANISH: **Teleprocesamiento (teleprocessing)**

Telnet Used to enable remote access to a server computer. Scope Note: Commands typed are run on the remote server.
SPANISH: **Telnet**

Terminal Access Controller Access Control System Plus (TACACS+) An authentication protocol, often used by remote-access servers.
SPANISH: **Sistema avanzado de control de acceso de controladores de acceso a terminales (TACACS+)**

Terms of reference A document that confirms the client's and the IS auditor's acceptance of a review assignment.
SPANISH: **Términos de referencia**

Test data Simulated transactions that can be used to test processing logic, computations and controls actually programmed in computer applications. Individual programs or an entire system can be tested. Scope Note: This technique includes Integrated Test Facilities (ITFs) and Base Case System Evaluations (BCSEs).
SPANISH: **Datos de prueba**

Test generators Software used to create data to be used in the testing of computer programs.
SPANISH: **Generadores de pruebas**

Test programs Programs that are tested and evaluated before approval into the production environment. Scope Note: Test programs, through a series of change control moves, migrate from the test environment to the production environment and become production programs.
SPANISH: **Programas de prueba**

Test types Test types include: (a) Checklist test--Copies of BCP is distributed to appropriate personnel for review
(b) Structured walk through--Identified key personnel walk through the plan to ensure that the plan accurately reflects the organization's ability to recover successfully
(c) Simulation test--All operational and support personnel are expected to perform an simulated emergency as a practice session
(d) Parallel Test--Critical systems are run at alternate site (hot, cold, warm or reciprocal)
(e) Complete interruption test--Disaster is replicated, normal production is shut down with real time recovery process.
SPANISH: **Tipos de pruebas**

Testing The examination of a sample from a population to estimate characteristics of the population.
SPANISH: **Pruebas**

Third-party review An independent audit of the control structure of a service organization, such as a service bureau, with the objective of providing assurances to the users of the service organization that the internal control structure is adequate, effective and sound.
SPANISH: **Revisión de terceros**

Threat Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm. Scope Note: A potential cause of an unwanted incident. (ISO/IEC 13335)
SPANISH: **Amenaza**

Threat agent Methods and things used to exploit a vulnerability. Scope Note: Examples include determination, capability, motive and resources.
SPANISH: **Agente de amenaza**

Threat analysis An evaluation of the type, scope and nature of events or actions that can result in adverse consequences; identification of the threats that exist against organization assets. Scope Note: The threat analysis usually also defines the level of threat and the likelihood of it materializing.
SPANISH: **Análisis de amenazas**

Threat event Any event where a threat element/actor acts against an asset in a manner that has the potential to directly result in harm
SPANISH: **Evento de amenaza**

Throughput The quantity of useful work made by the system per unit of time. Throughput can be measured in instructions per second or some other unit of performance. When referring to a data transfer operation, throughput measures the useful data transfer rate and is expressed in kbps, Mbps and Gbps.
SPANISH: **Rendimiento (throughput)**

Token A device that is used to authenticate a user, typically in addition to a username and password. Scope Note: A token is usually a credit card-sized device that displays a pseudo random number that changes every few minutes.
SPANISH: **Token**

Token ring topology A type of LAN ring topology in which a frame containing a specific format, called the token, is passed from one station to the next around the ring. Scope Note: When a station receives the token, it is allowed to transmit. The station can send as many frames as desired until a predefined time limit is reached. When a station either has no more frames to send or reaches the time limit, it transmits the token. Token passing prevents data collisions that can occur when two computers begin transmitting at the same time.
SPANISH: **Topología Token Ring**

Top-level management The highest level of management in the organization, responsible for direction and control of the organization as a whole (such as director, general manager, partner, chief officer and executive manager).
SPANISH: **Alta gerencia**

Topology The physical layout of how computers are linked together. Scope Note: Examples of topology include ring, star and bus
SPANISH: **Topología**

Total cost of ownership (TCO) Includes original cost of the computer and software, hardware and software upgrades, maintenance, technical support, training and certain activities performed by users.
SPANISH: **Costo total de propiedad (TCO)**

Transaction Business events or information grouped together because they have a single or similar purpose. Scope Note: Typically, a transaction is applied to a calculation or event that then results in the updating of a holding or master file.
SPANISH: **Transacción**

Transaction log A manual or automated log of all updates to data files and databases.
SPANISH: **Registro de transacciones (transaction log)**

Transaction protection Also known as "automated remote journaling of redo logs", a data recovery strategy that is similar to electronic vaulting, except that instead of transmitting several transaction batches daily, the archive logs are shipped as they are created.
SPANISH: **Protección de transacción**

Transmission Control Protocol (TCP) A connection-based Internet protocol that supports reliable data transfer connections. Scope Note: Packet data is verified using checksums and retransmitted if it is missing or corrupted. The application plays no part in validating the transfer.
SPANISH: **Protocolo de control de transmisión (TCP)**

Transmission Control Protocol/Internet Protocol (TCP/IP) Provides the basis for the Internet; a set of communications protocols that encompasses media access, packet transport, session communications, file transfer, electronic mail, terminal emulation, remote file access and network management.
SPANISH: **Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP)**

Transparency Refers to an enterprise's openness about its activities and is based on the concepts:

It is clear to those who are affected by or want to challenge governance decisions how the mechanism functions
A common vocabulary has been established
Relevant information is readily available Scope Note: Transparency and stakeholder trust are directly related; the more transparency in the governance process, the more confidence in the governance.
SPANISH: **Transparencia**

Trap door Unauthorized electronic exits, or doorways, out of an authorized computer program into a set of malicious instructions or programs.
SPANISH: **Puerta trasera en software (trap door)**

Trojan horse Purposefully hidden malicious or damaging code within an authorized computer program. Scope Note: Unlike viruses, they do not replicate themselves, but they can be just as destructive to a single computer.
SPANISH: **Caballo de Troya**

Trusted processes Processes certified as supporting a security goal.
SPANISH: **Procesos en que se confía**

Trusted systems Systems that employ sufficient hardware and software assurance measures to allow their use for processing of a range of sensitive or classified information.
SPANISH: **Sistemas en que se confía**

Tunnel The paths the encapsulated packets follow in an Internet VPN.
SPANISH: **Túnel**

Tunneling Commonly used to bridge between incompatible hosts/routers or to provide encryption, a method by which one network protocol encapsulates another protocol within itself. Scope Note: When protocol A encapsulates protocol B, then a protocol A header and optional tunneling headers are appended to the original protocol B packet. Protocol A then becomes the data link layer of protocol B. Examples of tunneling protocols include IPSec, Point-to-point Protocol Over Ethernet (PPPoE), and Layer 2 Tunneling Protocol (L2TP).
SPANISH: **Tunelización (tunneling)**

Tuple A row or record consisting of a set of attribute value pairs (column or field) in a relational data structure.
SPANISH: **Tupla**

Twisted pairs A low-capacity transmission medium, a pair of small, insulated wires that are twisted around each other to minimize interference from other wires in the cable.
SPANISH: **Pares trenzados**

Two-factor authentication The use of two independent mechanisms for authentication, for example, requiring a smart card and a password. Typically the combination of something you know, are or have.
SPANISH: **Autenticación de dos factores**

U

Unicode A standard for representing characters as integers. Scope Note: Unicode uses 16 bits, which means that it can represent more than 65,000 unique characters, as is necessary for languages such as Chinese and Japanese.
SPANISH: **Unicode**

Uninterruptible power supply (UPS) Provides short-term backup power from batteries for a computer system when the electrical power fails or drops to an unacceptable voltage level.
SPANISH: **Sistema de alimentación ininterrumpida (SAI, UPS)**

Unit testing A testing technique that is used to test program logic within a particular program or module. Scope Note: The purpose of the test is to ensure that the internal operation of the program performs according to specification. It uses a set of test cases that focus on the control structure of the procedural design.
SPANISH: **Pruebas unitarias**

Universal description, discovery and integration (UDDI) A web-based version of the traditional phone book's yellow and white pages enabling businesses to be publicly listed in promoting greater e-commerce activities.
SPANISH: **Descripción, descubrimiento e integración universal (UDDI)**

Universal Serial BUS (USB) An external bus standard that provides capabilities to transfer data at a rate of 12 Mbps. Scope Note: A USB port can connect up to 127 peripheral devices.
SPANISH: **Bus serial universal (USB)**

UNIX A multi-user, multitasking operating system that is used widely as the master control program in workstations and especially servers.
SPANISH: **UNIX**

Untrustworthy host The host is referred to as untrustworthy because it cannot be protected by the firewall; therefore, hosts on the trusted networks can place only limited trust in it. Scope Note: To the basic border firewall, add a host that resides on an untrusted network where the firewall cannot protect it. That host is minimally configured and carefully managed to be as secure as possible. The firewall is configured to require incoming and outgoing traffic to go through the untrustworthy host.
SPANISH: **Host poco confiable**

Uploading The process of electronically sending computerized information from one computer to another computer. Scope Note: When uploading, most often the transfer is from a smaller computer to a larger one.
SPANISH: **Subir (uploading)**

User awareness The training process in security-specific issues to reduce security problems, since users are often the weakest link in the security chain.
SPANISH: **Concienciación del usuario**

User Datagram Protocol (UDP) A connectionless Internet protocol that is designed for network efficiency and speed at the expense of reliability. Scope Note: A data request by the client is served by sending packets without testing to verify if they actually arrive at the destination, not if they were corrupted in transit. It is up to the application to determine these factors and request retransmissions.
SPANISH: **Protocolo de Datagrama de Usuario (UDP)**

Utility programs Specialized system software used to perform particular computerized functions and routines that are frequently required during normal processing. Scope Note: Examples of utility programs include sorting, backing up and erasing data.
SPANISH: **Programas de utilidad (utility programs)**

Utility script A sequence of commands input into a single file to automate a repetitive and specific task. Scope Note: The utility script is executed, either automatically or manually, to perform the task. In Unix, these are known as shell scripts.
SPANISH: **Script de utilidad (utility script)**

Utility software Computer programs provided by a computer hardware manufacturer or software vendor and used in running the system. Scope Note: This technique can be used to examine processing activities; to test programs, system activities and operational procedures; to evaluate data file activity; and, to analyze job accounting data.
SPANISH: **Software de utilidad**

V

Vaccine A program designed to detect computer viruses.
SPANISH: **Vacuna**

Val IT The standard framework for organizations to select and manage IT-related business investments and ITassets by means of investment programs such that they deliver the optimal value to the organization. Based on COBIT.
SPANISH: **Val IT**

Validity check Programmed checking of data validity in accordance with predetermined criteria.
SPANISH: **Verificación de validez (validity check)**

Value The relative worth or importance of an investment for an organization, as perceived by its key stakeholders, expressed as total life cycle benefits net of related costs, adjusted for risk and (in the case of financial value) the time value of money.
SPANISH: **Valor**

Value-added network (VAN) A data communication network that adds processing services such as error correction, data translation and/or storage to the basic function of transporting data.
SPANISH: **Red de valor añadido (value added network)**

Variable sampling A sampling technique used to estimate the average or total value of a population based on a sample; a statistical model used to project a quantitative characteristic, such as a monetary amount.
SPANISH: **Muestreo de variables**

Verification Checks that data are entered correctly.
SPANISH: **Verificación**

Virtual organizations Organizations that have no official physical site presence and are made up of diverse, geographically dispersed or mobile employees.
SPANISH: **Organizaciones virtuales**

Virtual private network (VPN) A secure private network that uses the public telecommunications infrastructure to transmit data. Scope Note: In contrast to a much more expensive system of owned or leased lines that can only be used by one company, VPNs are used by enterprises for both extranets and wide areas of intranets. Using encryption and authentication, a VPN encrypts all data that pass between two Internet points, maintaining privacy and security.
SPANISH: **Redes virtuales privadas (VPN)**

Virus A program with the ability to reproduce by modifying other programs to include a copy of itself. Scope Note: A virus may contain destructive code that can move into multiple programs, data files or devices on a system and spread through multiple systems in a network.
SPANISH: **Virus**

Virus signature files The file of virus patterns that are compared with existing files to determine if they are infected with a virus or worm.
SPANISH: **Archivos de firma de virus**

Voice mail A system of storing messages in a private recording medium where the called party can later retrieve the messages.
SPANISH: **Correo de voz**

Voice-over Internet Protocol (VoIP) Also called IP Telephony, Internet telephony and Broadband Phone, this is a technology that makes it possible to have a voice conversation over the Internet or over any dedicated Internet Protocol (IP) network instead of dedicated voice transmission lines.
SPANISH: **Voz por protocolo de Internet (VoIP)**

Vulnerability A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events
SPANISH: **Vulnerabilidad**

Vulnerability analysis Process of identifying and classifying vulnerabilities.
SPANISH: **Análisis de vulnerabilidades**

Vulnerability event Any event where a material increase in vulnerability results.
that this increase in vulnerability can result from changes in control conditions or from changes in threat capability/force. Scope Note: From Jones, J.; "FAIR Taxonomy," Risk Management Insight, USA, 2008.
SPANISH: **Evento de vulnerabilidad**

W

Walk-through A thorough demonstration or explanation that details each step of a process.
SPANISH: **Recorrido (walk-through)**

WAN switch A data link layer device used for implementing various WAN technologies such as asynchronous transfer mode, point-to-point frame relay solutions, and ISDN. Scope Note: WAN switches are typically associated with carrier networks providing dedicated WAN switching and router services to organizations via T-1 or T-3 connections.
SPANISH: **Switch WAN**

War dialer Software packages that sequentially dial telephone numbers, recording any numbers that answer.
SPANISH: **Marcado automático de números telefónicos empleando un módem (War dialer)**

Warm site Similar to a hot site; however, it is not fully equipped with all necessary hardware needed for recovery.
SPANISH: **Warm site**

Waterfall development Also known as traditional development, it is a procedure-focused development cycle with formal sign-off at the completion of each level.
SPANISH: **Desarrollo en cascada**

Web hosting The business of providing the equipment and services required to host and maintain files for one or more web sites and provide fast Internet connections to those sites. Scope Note: Most hosting is "shared" which means that web sites of multiple companies are on the same server to share/reduce costs.
SPANISH: **Alojamiento web**

Web page A viewable screen displaying information, presented through a web browser in a single view, sometimes requiring the user to scroll to review the entire page. Scope Note: An enterprise's web page may display the enterprise’s logo, provide information about the enterprise's products and services, or allow a customer to interact with the enterprise or third parties that have contracted with the enterprise.
SPANISH: **Página web**

Web server Using the client-server model and the World Wide Web's Hypertext Transfer Protocol (HTTP), Web server is a software program that serves web pages to users.
SPANISH: **Servidor web**

Web Services Description Language (WSDL) An XML-formatted language used to describe a web service's capabilities as collections of communication endpoints capable of exchanging messages; WSDL is the language that UDDI uses. Also see Universal Description, Discovery and Integration (UDDI).
SPANISH: **Lenguaje de descripción de servicios web (WSDL)**

Web site Consists of one or more web pages that may originate at one or more web server computers. Scope Note: A person can view the pages of a web site in any order, as he/she would a magazine.
SPANISH: **Sitio web**

White box testing A testing approach that uses knowledge of a program/module’s underlying implementation and code intervals to verify its expected behavior.
SPANISH: **Pruebas de caja blanca (white box testing)**

Wide area network (WAN) A computer network connecting different remote locations that may range from short distances, such as a floor or building, to extremely long transmissions that encompass a large region or several countries.
SPANISH: **Red de área amplia (WAN)**

Wi-Fi Protected Access (WPA) A class of systems used to secure wireless (Wi-Fi) computer networks. Scope Note: WPA was created in response to several serious weaknesses researchers found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards. Both provide good security with two significant issues. First, either WPA or WPA2 must be enabled and chosen in preference to WEP; WEP is usually presented as the first security choice in most installation instructions. Second, in the “personal” mode, the most likely choice for homes and small offices, a pass phrase is required that, for full security, must be longer than the typical 6 to 8 character passwords users are taught to employ.
SPANISH: **Acceso Wi-Fi protegido (WPA)**

Windows NT A version of the Windows operating system that supports preemptive multitasking.
SPANISH: **Windows NT**

Wired Equivalent Privacy (WEP) A scheme that is part of the IEEE 802.11 wireless networking standard to secure IEEE 802.11 wireless networks (also known as Wi-Fi networks). Scope Note: Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping. WEP was intended to provide comparable confidentiality to a traditional wired network (in particular it does not protect users of the network from each other), hence the name. Several serious weaknesses were identified by cryptanalysts, and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004. Despite the weaknesses, WEP provides a level of security that can deter casual snooping.
SPANISH: **Privacidad Equivalente al Cableado (WEP)**

Wireless computing The ability of computing devices to communicate in a form to establish a local area network without cabling infrastructure (wireless), and involves those technologies converging around IEEE 802.11 and 802.11b and radio band services used by mobile devices.
SPANISH: **Computación inalámbrica**

Wiretapping The practice of eavesdropping on information being transmitted over telecommunications links.
SPANISH: **Intercepción de información por cable (wiretapping)**

World Wide Web (WWW) A sub network of the Internet through which information is exchanged by text, graphics, audio and video.
SPANISH: **World Wide Web (WWW)**

World Wide Web Consortium (W3C) An international consortium founded in 1994 of affiliates from public and private organizations involved with the Internet and the web. Scope Note: The W3C's primary mission is to promulgate open standards to further enhance the economic growth of Internet web services globally.
SPANISH: **World Wide Web Consortium (W3C)**

Worm Programmed network attacks in which a self-replicating program does not attach itself to programs, but rather spreads independently of users' actions.
SPANISH: **Gusano**

X

X.25 A protocol for packet-switching networks.
SPANISH: **X.25**

X.25 Interface An interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode on some public data networks.
SPANISH: **Interfaz X.25**

X.500 Standard that defines how global directories should be structured. Scope Note: X.500 directories are hierarchical with different levels for each category of information, such as country, state and city.
SPANISH: **X.500**