GTAG

GUÍA DE AUDITORÍA DE TECNOLOGÍA GLOBAL

Gestión y auditoría de puntos vulnerables de tecnología de la información

The Institute of Internal Auditors

Guía de Auditoría de Tecnología Global (GTAG) 6: Gestión y auditoría de puntos vulnerables de tecnología de la información

Autores:

Sasha Romanosky, Escuela de Política y Administración Pública Heinz de la Universidad Carnegie Mellon

Gene Kim, Tripwire Inc. e IT Process Institute

Bridget Kravchenko, General Motors Corp.

Octubre 2006

GTAG — Índice

1 Resumen ejecutivo 1
2 Introducción 2
2.1 Identificar una gestión de puntos vulnerables deficiente 2
2.2 Mejorar la gestión de puntos vulnerables 2
2.3 El rol del auditor interno 2
2.4 De qué manera la gestión de puntos vulnerables impulsa determinados cambios en la infraestructura de TI 2
3 Ciclo de vida de la gestión de puntos vulnerables 4
3.1 Identificación y validación 4
Sistemas de determinación de alcance
Detectar vulnerabilidades
Validar los hallazgos
3.2 Evaluación de riesgos y establecimiento de prioridades 5
Evaluación de riesgos
Establecer prioridades entre las vulnerabilidades
3.3 Enmiendas 5
Mitigar vulnerabilidades críticas
Crear proceso para mitigar vulnerabilidades
3.4 Mejora continua 6
Detener la propagación
Fijar las expectativas en función de los Acuerdos de nivel de operaciones (OLA, en inglés)
Lograr la eficiencia a través de la automatización
Usar las experiencias pasadas para guiar las acciones futuras
4 Madurez de la organización 7
4.1 Organizaciones de bajo rendimiento 7
4.2 Organizaciones de alto rendimiento 8
5 Apéndice 10
5.1 Métricas 10
5.2 Las diez preguntas principales que los DEA deben realizar sobre gestión de puntos vulnerables 11
5.3 Unas palabras sobre la gestión de riesgos y puntos vulnerables 13
5.4 Recursos del auditor interno para combatir las vulnerabilidades 13
5.5 Glosario 15
6 Referencias 16
7 Acerca de los autores 17
Revisores

Los autores desean agradecer a Julia Allen, Lily Bi, Ron Gula, George Spafford y a muchos otros revisores que proporcionaron una retroalimentación muy valiosa. Un agradecimiento especial a Peter Mell del Instituto Nacional de Normas y Tecnología (NIST, en inglés) de Estados Unidos por sus invaluables contribuciones.

Entre otras responsabilidades, las áreas de gestión y seguridad de TI tienen a su cargo la tarea de asegurar que los riesgos de la tecnología se gestionen apropiadamente. Esos riesgos se originan en la implementación y el uso de los activos de TI de distintas maneras, como por ejemplo, configurar sistemas de modo incorrecto u obtener acceso a software restringido. Sin embargo, estos riesgos se pueden identificar y solucionar identificando vulnerabilidades, evaluando su impacto potencial e implementando medidas correctivas, cuando ellas estén garantizadas.

La gestión de puntos vulnerables consiste en los procesos y las tecnologías que una organización emplea para identificar, evaluar y solucionar las vulnerabilidades de TI (debilidades o exposiciones en los activos o procesos de TI que pueden generar un riesgo de negocio[1] o un riesgo de seguridad[2]). Según la Base de Datos del Gobierno de EE. UU. sobre Vulnerabilidades (NVD, en inglés)[3], se descubren aproximadamente 5.000 nuevas vulnerabilidades cada año y el 40% de ellas son de "alta gravedad" (es decir, podrían provocar interrupciones en las principales operaciones de las organizaciones).

Tal vez, usted se esté preguntando por qué debe leer una guía sobre gestión de puntos vulnerables. Al fin y al cabo, ¿no es ese un asunto que puede delegar por completo en su personal de auditoría de TI? La respuesta es "no". Con frecuencia, el impacto potencial de un riesgo relacionado con la TI no se define ni se comprende correctamente hasta que un gusano, como por ejemplo el SQL Slammer, cierra definitivamente las operaciones de negocios. Saber cómo educar e informar a la dirección ejecutiva sobre la importancia de la gestión de puntos vulnerables ayudará a obtener el respaldo y generar un llamado para la acción. La dirección ejecutiva debe entender que para tener un programa eficaz de gestión de puntos vulnerables, primero es necesario diseñar un proceso para detectar, evaluar y mitigar las vulnerabilidades de manera continua, integrando esas tareas en el enfoque general de proceso de TI. No todas las cuestiones relacionadas con la gestión de puntos vulnerables son de naturaleza técnica. En realidad, muchos de los grandes desafíos radican en motivar a las personas y en impulsar procesos eficaces.

Esta guía fue desarrollada para ayudar a los directores ejecutivos de auditoría (DEA, en inglés) a formular las preguntas correctas al personal de seguridad de TI, cuando evalúan la eficacia de sus procesos de gestión de puntos vulnerables. La guía recomienda prácticas de gestión específicas para asistir a la organización en el logro y sostenimiento de altos niveles de eficacia y eficiencia, a la vez que ilustra las diferencias entre los esfuerzos, de alto y bajo rendimiento, de gestión de puntos vulnerables.

Después de leer esta guía, usted podrá realizar lo siguiente:

- Tener conocimiento práctico de los procesos de gestión de puntos vulnerables.
- Tener la habilidad de poder diferenciar entre organizaciones de alto y bajo rendimiento en cuanto a gestión de puntos vulnerables.
- Familiarizarse con el avance típico de niveles de capacidad, desde un enfoque basado en la tecnología, a un enfoque basado en el riesgo y, por último, a un enfoque basado en un proceso de TI.
- Proporcionar una guía útil a la dirección de TI sobre mejores prácticas para la gestión de puntos vulnerables.
- Poder vender sus recomendaciones más eficazmente al Director de TI (DTI), Director de Seguridad de la Información (CISO, en inglés), Presidente (CEO) y al Director Financiero (CFO, en inglés).

[1] Como por ejemplo, no poder mantener la integridad de los informes financieros o pérdida de ganancias o productividad.
[2] Como por ejemplo, violaciones a la confidencialidad, integridad o disponibilidad de datos.
[3] http://nvd.nist.gov

Las vulnerabilidades de TI se han convertido en una epidemia y exponen las redes a ataques, virus y gusanos. De hecho, diariamente se descubren más de 12 vulnerabilidades en los productos de hardware y software[4] .Otros tipos de vulnerabilidades de TI son, por ejemplo, la gestión inadecuada de contraseñas, el acceso inapropiado a archivos, una criptografía débil y aplicaciones mal configuradas. Mantenerse al día con los últimos anuncios y parches se ha convertido en un trabajo sin interrupciones para los gerentes de TI y los profesionales de seguridad. Sin embargo, algunos tienen más éxito que otros.

2.1 Identificar una gestión de puntos vulnerables deficiente

Los seis indicadores principales de procesos deficientes de gestión de puntos vulnerables son los siguientes:

- Cantidad de incidentes de seguridad más alta que lo aceptable[5] durante un período dado.
- Incapacidad para identificar vulnerabilidades de TI de manera sistemática, lo cual ocasiona la exposición de activos críticos.
- Incapacidad para evaluar los riesgos asociados a cada punto vulnerable y para establecer prioridades entre las actividades de mitigación de las vulnerabilidades.
- Relaciones laborales deficientes entre la gestión de TI y la seguridad de TI, lo cual conduce a una incapacidad para controlar y realizar cambios en los activos informáticos.
- Falta de un sistema de gestión de activos.
- Falta de un proceso de gestión de configuración que se integre con los esfuerzos de mitigación de vulnerabilidades.

2.2 Mejorar la gestión de puntos vulnerables

Los seis pasos prescriptivos que se pueden adoptar para mejorar los procesos de gestión de puntos vulnerables son los siguientes:

- Obtener el respaldo de la dirección ejecutiva para identificar y solucionar las vulnerabilidades de TI de manera coherente con el grado de tolerancia al riesgo de la organización.
- Obtener un inventario completo de todos los activos de TI y sus vulnerabilidades.
- Establecer prioridades entre los esfuerzos para implementar enmiendas en función de los riesgos de negocio.
- Solucionar las vulnerabilidades proporcionando proyectos de trabajos planeados a la dirección de TI.
- Actualizar permanentemente la detección de activos[6], las pruebas de vulnerabilidad y los procesos de enmienda.
- Utilizar, al máximo grado posible, tecnologías automatizadas de gestión de parches y detección de vulnerabilidades.

2.3 El rol del auditor interno

La gestión de puntos vulnerables se ha convertido en una prioridad principal dado que los controles de TI se consideran parte de la estructura de control interno sobre los informes financieros y los requisitos de cumplimiento de las regulaciones provenientes, por ejemplo, de la Ley Sarbanes-Oxley de 2002, del Consejo Federal de Examen de las Instituciones Financieras (FFIEC)[7] y de las leyes SOX en sus versiones canadiense y japonesa. En consecuencia, cada vez más, la gestión de TI debe prestar servicios esenciales para la misión de los negocios. La gestión y la seguridad de TI son responsables de implementar y demostrar que existen suficientes controles de seguridad y que estos funcionan eficazmente para satisfacer los requisitos reglamentarios y de control interno.

Los auditores internos sirven de guía y proporcionan valor a los negocios de diferentes maneras. Pueden evaluar la eficacia de las medidas preventivas, de detección y de mitigación puestas en práctica contra ataques pasados, según sea apropiado, y también futuros ataques o incidentes que probablemente puedan ocurrir. Deben confirmar que se ha informado apropiadamente al consejo de administración sobre amenazas, incidentes, vulnerabilidades y medidas correctivas.

También, deben brindar recomendaciones a la dirección ejecutiva respecto del cumplimiento de requerimientos reglamentarios e internos, a la vez que impulsan su toma de conciencia sobre probables vulnerabilidades e impactos. De esta manera, los auditores internos ayudan a la dirección ejecutiva a identificar posibles fuentes de riesgo para la empresa, al mismo tiempo que contribuyen a evitar incidentes de seguridad o incumplimientos reglamentarios. En especial, identifican los lugares donde la seguridad de TI ha fallado en la implementación de procesos eficaces de gestión de puntos vulnerables y validan los esfuerzos de enmiendas de vulnerabilidades existentes.

Tal vez los auditores se podrían preguntar "¿Cómo se vería el alcance de una auditoría de puntos vulnerables?" La Tabla 1 proporciona una breve introducción sobre las actividades que los auditores pueden considerar dentro de tal alcance. En la Sección 3, se pueden obtener más detalles de cada parte de esta tabla.

2.4 De qué manera la gestión de puntos vulnerables impulsa determinados cambios en la infraestructura de TI

Las tareas de escanear y descubrir vulnerabilidades dan inicio al proceso de evaluación de riesgos, que posiblemente, a su turno, demanden cambios en los activos de TI. Dada la proliferación de vulnerabilidades cada vez más intensa, la ejecución exitosa del proceso que va desde la detección a la implementación de enmiendas de manera expeditiva es importante para garantizar que el impacto sobre el negocio sea mínimo. Esto implica que la gestión de puntos vulnerables debe estar integrada a las actividades de gestión de parches y cambios de la organización. Tal como se analizará más abajo, establecer prioridades y ejecutar los cambios en los activos de TI siempre es un desafío, pero hay maneras de determinar si usted cuenta con un proceso eficaz de gestión de puntos vulnerables que está totalmente integrado con las prácticas de gestión del cambio de la organización. Los procesos de gestión del cambio se analizan en detalle en la guía *GTAG 2: Controles de gestión de parches y cambios*. [5]

[4] Fuente: Base de datos nacional de vulnerabilidades (NVD, en inglés)

[5] La cantidad "aceptable" de incidentes se puede determinar comparando la tolerancia a la pérdida de uno, con la pérdida proveniente de incidentes de experiencias anteriores. De esta manera, uno puede ajustar los esfuerzos de gestión de puntos vulnerables balanceando los costos de implementar controles y enmendar vulnerabilidades con los beneficios de estas actividades, posiblemente como una función de pérdida que se evitó.

[6] Este punto se analizará en la Sección 3.1.

[7] http://www.ffiec.gov

Identificación y validación	Evaluación de riesgos y establecimiento de prioridades	Enmiendas	Mantenimiento y mejoras
Invetario de activos Asegurarse de que se lleve y se mantenga un inventario de todos los sistemas de TI. Asegurarse de que los sistemas de TI identificados estén agrupados y que se establezcan prioridades según sus riesgos de negocio correspondientes. Asegurarse de que haya dependencias de proceso entre la gestión de configuración y la gestión del cambio.	**Evaluaciones de riesgos** Identificar los criterios utilizados para asignar los riesgos a medida que se detectan las vulnerabilidades. Asegurarse de que los criterios se utilizan en forma coherente en toda la organización.	**Supervisión** IIdentificar los procesos automatizados y manuales para anuncios de vulnerabilidades. Desarrollar planes de contingencia para el caso en que una vulnerabilidad identificada no reciba el parche adecuado a tiempo.	**Gestión de configuración** Asegurarse de que los activos de TI sean mantenidos en un formato estandarizado para ayudar a rastrear los elementos físicos y lógicos del activo de TI, como por ejemplo, modelos, aplicaciones instaladas y parches. Asegurarse de que la gestión del cambio y de incidentes e stén integradas con la gestión de configuración.
Detección de vulnerabilidades Identificar herramientas automatizadas utilizadas para escanear y supervisar la red y los dispositivos host. Asegurarse de que los activos de TI se escaneen periódicamente. Identificar las fuentes utilizadas para la información de vulnerabilidades oportuna (por ejemplo, terceros, proveedores de softwate, CERT).	**Establecer prioridades entre vulnerabilidades** Analizar de qué manera se cuantifica la significancia en función del impacto y criticidad del sistema. Asegurarse de que el impacto de negocio se incluya como un identificador de prioridad medible.	**Gestión de incidentes** Los procedimientos de enmiendas deben ser coherentes en toda la organización. El impacto y la urgencia asignados a los tiques de incidentes deben estar en línea con el riesgo de negocio del activo. Las métricas de incidentes, como por ejemplo, tiempo medio de recuperación, deben ser definidas y rastreadas para asegurarse de que se cumplan los acuerdos de nivel de operaciones (OLA, en inglés).	**Acuerdos de nivel de operaciones** Identificar que haya acuerdos de nivel de operaciones implementados para asegurarse que el ritmo de la gestión de puntos vulnerables y las entregas de procesos se midan y tengan una persona a cargo responsable.
Validación de los hallazgos Asegurarse de que hay un proceso implementado para identificar falsos positivos y negativos durante la detección. Asegurarse de que se analicen las vulnerabilidades según corresponda al entorno nativo.		**Gestión del cambio** Analizar si los cambios son reactivos ante las vulnerabilidades identificadas. Los parches se deben planificar y probar antes de su implementación.. Los cambios que se producen como resultado de vulnerabilidades deben ocasionar el mínimo grado de interrupciones en el negocio.	**Políticas y requerimientos** Asegurarse de que los roles y las responsabilidades estén definidos para las funciones de identificación, comunicación y enmienda. Identificar las políticas y los procedimientos para asegurarse de que se hayan definido las estrategias y las decisiones apropiadas.
		Prueba de parches Determinar cómo se implementan los parches centralizados para asegurar su eficiencia y eliminar esfuerzos duplicados para la misma vulnerabilidad. Asegurarse de que se prueben y verifiquen los parches para detectar virus. Asegurarse de que los parches se prueben en un entorno de preproducción para garantizar que no habrá riesgos inesperados ni problemas de impacto en el servicio a raíz de tales parches [5]. Identificar procedimientos de parches automatizados y manuales para asegurarse la eficiencia de su implementación.	

Tabla 1: Alcance de la auditoría de gestión de puntos vulnerables

Esta sección describe sólo los componentes críticos necesarios para lograr un programa eficaz de gestión de puntos vulnerables. Para obtener un análisis más amplio, consulte la publicación *Creating a Patch and Vulnerability Management Program* [3].

En la Figura 1 se ilustran las dependencias entre las funciones relevantes de la seguridad de TI y las operaciones de TI. A los fines de este documento, consideramos las funciones de una organización que implementa el enfoque de IT Infrastructure Library (ITIL) [8].

El Ciclo de vida de la gestión de puntos vulnerables comienza por identificar los activos de TI para luego escanearlos o supervisarlos con el fin de identificar las debilidades de TI. Esos datos respecto de vulnerabilidades entonces se validan para confirmar que, en efecto, tales vulnerabilidades existen. Posteriormente, se establecen las prioridades en función del riesgo para la organización.

Las vulnerabilidades críticas están a cargo de Gestión de incidentes, quien coordina los esfuerzos de enmienda con Gestión del cambio utilizando procedimientos de cambios de emergencia que aceleran la implementación en producción. Las vulnerabilidades no críticas se revisan por medio del proceso estándar de Gestión del cambio. Una vez aprobado, Gestión de liberaciones prepara, prueba y facilita el cambio. Nuevamente, Gestión del cambio revisa el cambio para garantizar que cumple con todos los requerimientos y, finalmente, la base de datos de Gestión de configuración es actualizada para reflejar esas modificaciones de mejora (por ejemplo, mayor seguridad).

Observe que independientemente de que el trabajo de enmienda sea una emergencia o no, todos los cambios se procesan a través de Gestión del cambio. Ellos actúan cumpliendo un rol organizador para impulsar el cambio a través de la maquinaría de TI a fin de lograr su implementación exitosa.

3.1 Identificación y validación

Sistemas de determinación de alcance

Para determinar el alcance de los sistemas adecuadamente, el auditor debe obtener una lista completa de todos los segmentos de red usados a través de la organización, como por ejemplo, redes corporativas cableadas e inalámbricas, redes de producción, redes de administración y respaldo, redes de tránsito, redes de laboratorios y pruebas, y oficinas remotas. Se debe identificar y documentar cada una de estas redes.

Las redes también deben incluirse en un diagrama de arquitectura de red que muestre las interconexiones, además de los dispositivos de seguridad perimetral, como por ejemplo, enrutadores, filtros de seguridad y sistemas de detección de intrusiones. Este diagrama le permitirá a la dirección entender cómo un punto vulnerable detectado en una red puede ejercer un impacto sobre la seguridad de los activos de otra red.

Detectar vulnerabilidades

Una vez obtenido el inventario de la red, todos los activos de TI conectados a cada segmento de red deberían escanearse o supervisarse periódicamente para detectar posibles vulnerabilidades. Entre esos activos se incluyen dispositivos como los servidores de aplicaciones de negocio (por ejemplo, servidores Web, de base de datos, de correo electrónico y de gestión de

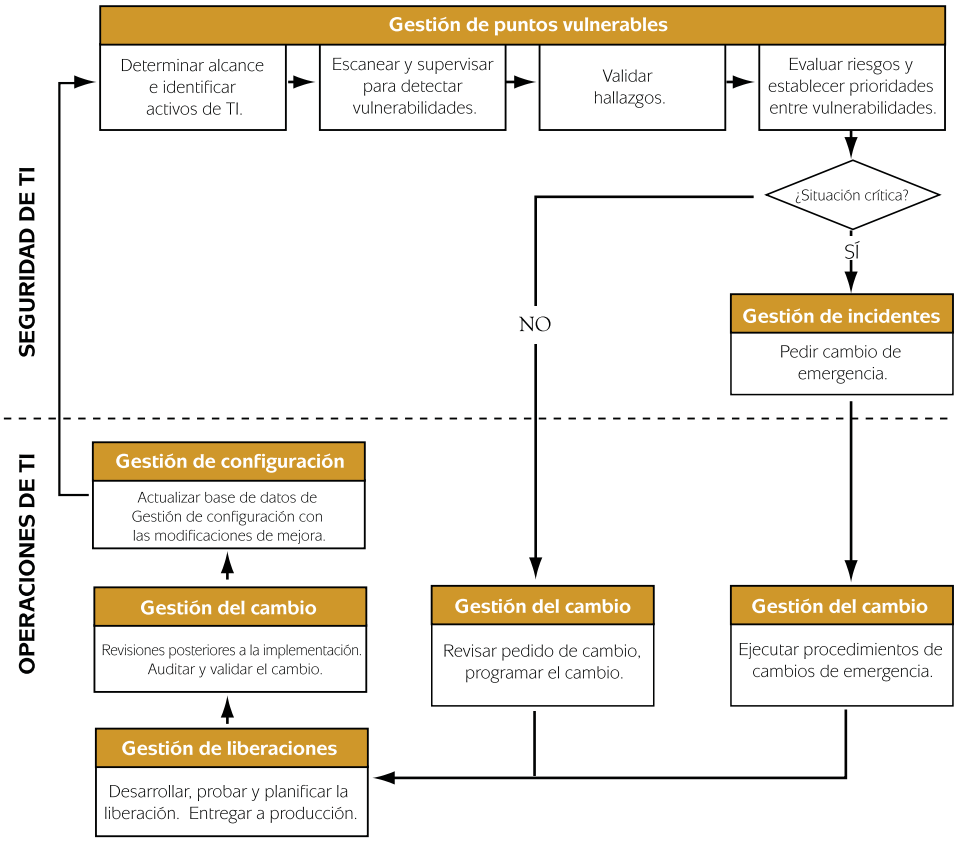

Figura 1: Gestión de puntos vulnerables y dependencias de TI

relaciones de clientes), los dispositivos de seguridad, de redes de contacto, de telecomunicaciones y las impresoras.

La acción de escanear se refiere a dispositivos de red o aplicaciones especiales que examinan activamente otras aplicaciones y activos de TI para identificar debilidades[8]. Estos dispositivos deben estar programados para ejecutarse con una frecuencia diaria, mensual o trimestral según las necesidades, los riesgos o las capacidades de la organización[9].

La acción de supervisar se refiere a agentes de software instalados en los activos de TI que suministran información de configuración de host. También, se refiere a dispositivos de red que de manera permanente escuchan el tráfico de red e informan, u opcionalmente bloquean, el tráfico malicioso que puede sacar provecho de una vulnerabilidad. Estos dispositivos son útiles para identificar activos de TI falsos o anteriormente desconocidos. Además, se consideran un control de seguridad preventivo dada su habilidad de bloquear los ataques antes de que provoquen pérdidas.

Validar los hallazgos

Por último, las empresas deben validar los resultados obtenidos de los procesos de escaneo y supervisión de vulnerabilidades. Si bien los dispositivos de escaneo y supervisión generalmente son buenos en cuanto a sofisticación y precisión, siempre tienen limitaciones. Pueden ocurrir errores en forma de "falsos positivos" o "falsos negativos". Un falso positivo es una vulnerabilidad que se ha informado pero no existe, debido a que el mecanismo de detección tuvo un error. Un falso negativo ocurre cuando el punto vulnerable existe, pero el sistema no pudo identificarlo.

3.2 Evaluación de riesgos y establecimiento de prioridades

Evaluación de riesgos

Una vez adquiridos los datos de las vulnerabilidades, la organización debe poder determinar el riesgo real que estos representan. Aunque generalmente no es necesario disponer de un proyecto de gestión de riesgos total, sí se necesita una evaluación de riesgos básica[10]. Dada la gran cantidad de vulnerabilidades detectadas en cada escaneo, es probable que la organización deba realizar un gran número de evaluaciones de miniriesgos. En consecuencia, la organización debe tener un procedimiento bien definido para medir los riesgos, que sea aplicable de manera rápida y precisa[11]. Observe que la presencia de un punto vulnerable, no siempre implica una enmienda puesto que la organización puede optar por aceptar el riesgo que presenta ese punto vulnerable [2], por ejemplo, cuando los controles de seguridad existentes reducen adecuadamente la probabilidad de que un ataque sea exitoso o cuando el activo, blanco del ataque, es de escaso valor o ninguno. En esos casos, la aceptación del riesgo se debe documentar y aprobar para evitar que el mismo hallazgo se vuelva a evaluar en otra oportunidad posterior.

Establecer prioridades entre las vulnerabilidades

La organización debe establecer las prioridades de enmienda de puntos vulnerables en función de la criticidad del activo vulnerable, de la probabilidad o frecuencia de que ocurra un ataque (por ejemplo, los dispositivos con acceso a Internet tienen más probabilidades de ser atacados que los dispositivos internos) y del esfuerzo que requiere la implementación de la corrección. De este modo, los auditores compararan el riesgo real que esa vulnerabilidad representa para la organización[12] con el costo de implementación de la corrección y establecerán la prioridad del riesgo en función de su eficacia con relación al costo. La organización también puede desear examinar las causas de los incidentes de seguridad anteriores y establecer las prioridades en función de ellos. Por ejemplo, tal vez los incidentes pasados fueron provocados por brechas iniciadas desde conexiones de terceros o fueron ocasionados por un software malicioso incorporado por los empleados.

3.3 Enmiendas

Mitigar las vulnerabilidades críticas

A menudo, la mejor manera de corregir las vulnerabilidades más críticas es que el personal de seguridad de TI utilice el incidente ya existente o los tiques de detección de problemas[13]. Este sistema probablemente sea parte de un procedimiento operativo estándar de TI, que asegura que el personal apropiado aborde la implementación de correcciones de manera oportuna.

Crear un proceso para mitigar las vulnerabilidades

La acción de corregir las vulnerabilidades más críticas elimina los peligros evidentes. Este debiera ser un proceso rápido de ejecutar, dado que puede haber sólo un par de vulnerabilidades Sin embargo, diferentes desafíos surgen cuando se intenta enmendar cientos o miles de vulnerabilidades de una sola vez. La manera más eficiente de ejecutar estas enmiendas es crear un proyecto de TI que incluya un gerente de proyecto, entregas de procesos y fechas límite. El proyecto entonces debe tener la autoridad como para integrarse con el proceso de gestión de configuración de la organización y para implementar los parches necesarios. Implementar un proyecto de gestión de puntos vulnerables bien diseñado con un proceso de gestión de configuración es el mejor modo de lograr una gestión de puntos vulnerables repetible y eficaz.

Como analogía, considere el equipo de desarrollo de una empresa de software de aplicación. El ciclo de vida del desarrollo de las aplicaciones se crea para producir software de calidad. Los equipos de desarrollo saben que nuevas características se identifican y solicitan para el desarrollo de productos. El equipo toma estas características, establece las prioridades en función del esfuerzo y valor para el negocio, y desarrolla, prueba e implementa el producto. Todo esto se realiza utilizando un proceso probado y maduro donde todos los interesados aceptan

[8] IT Infrastructure Library (ITIL) es un enfoque que describe las mejores prácticas para las organizaciones de servicios de TI de alto rendimiento.

[9] En una situación ideal, la información de los dispositivos debe estar dentro de una Base de Datos de Gestión de Configuración (CMDB, en inglés), pero en la práctica, puede ocurrir que la base de datos no siempre refleje lo que realmente está conectado a la red.

[10] En la Sección 5.4, se puede ver un ejemplo de un informe de escaneo de vulnerabilidades.

[11] La organización debe programar estos escaneos en función de su capacidad de procesamiento de la información de vulnerabilidades que se reúna. No tiene objeto programar escaneos con una frecuencia mayor que esa capacidad.

[12] Consulte la Sección 5.3 del Apéndice para obtener un análisis breve de la gestión de riesgos.

[13] Una métrica cuantitativa de tal naturaleza es el Sistema de Calificación de Vulnerabilidades Comunes (www.first.org/cvss).

sus motivaciones, roles y responsabilidades. Por ejemplo, un equipo de desarrollo puede solicitar una infraestructura adicional al personal de TI para respaldar una aplicación de negocio. Naturalmente, el departamento de TI puede mostrar cierta resistencia en cuanto a costos, fecha de entrega o configuración, pero las metas y expectativas son claras.

El éxito de un programa eficaz de gestión de puntos vulnerables radica en que el personal de seguridad de TI tenga una relación similar con la dirección de TI. Tal éxito también depende de que el trabajo de gestión de puntos vulnerables se formule y se entregue a la dirección de TI como otro componente de trabajo planificado[14] que se debe agregar a su carga normal de trabajo. Los detalles del proyecto, como por ejemplo, la fecha de entrega, las responsabilidades y la validación de vulnerabilidades, se vuelven, entonces, parte de la gran maquinaria de procesos y operaciones diarias de TI.

3.4 Mejora continua

Detener la propagación
Dado que las vulnerabilidades son tratadas a través de procesos de negocio de TI estándar, la Seguridad de TI debe notificar a Gestión del cambio sobre cualquier modificación permanente de sistemas o aplicaciones para garantizar que las futuras versiones se lancen al mercado con configuraciones más seguras. Esta notificación es crítica y es uno de los pocos pasos proactivos de la gestión de puntos vulnerables. Para asegurar que esta comunicación efectivamente se produzca, la organización de seguridad debe tener una relación directa con Gestión del cambio o con quienes sean los que administren el escritorio, el servidor y las versiones de aplicaciones.

Fijar las expectativas en función de los Acuerdos de nivel de operaciones (OLA, en inglés)
Las enmiendas eficaces de vulnerabilidades a menudo se hacen más complejas y difíciles dado que el grupo que detecta tales vulnerabilidades (o sea, Seguridad de TI), generalmente, no es el grupo que administra el activo de TI (Gestión de TI).

Frecuentemente, Seguridad de TI tal vez rastree adecuadamente las vulnerabilidades críticas de negocio, pero es posible que no tenga la capacidad de movilizar las operaciones de TI para abordarlas oportunamente. Por consiguiente, se debe establecer un OLA[15] para poder gestionar las expectativas de ambos grupos: los que emiten los pedidos y los que proporcionan el servicio. El OLA puede definir procedimientos por separado para cada categoría de vulnerabilidades. La Tabla 2 identifica un posible acuerdo.

Gravedad de la vulnerabilidad	Plazo para enmienda
1	2 días hábiles
2	5 días hábiles
3	15 días hábiles

Tabla 2: Ejemplo de acuerdo de enmiendas

Lograr la eficiencia a través de la automatización
La automatización mejora significativamente la eficiencia del grupo de gestión de puntos vulnerables. Cuánto más automatización en los procesos pueda tener la organización, como por ejemplo, escaneos de vulnerabilidades, creación de tiques con los grupos operativos, actualización de informes de estado y elaboración de informes; más podrá la organización centrarse en mejorar y escalar sus esfuerzos, o incluso, verdaderamente, destinar menos recursos a la seguridad de TI. Quienquiera sea el responsable de implementar los parches, debe utilizar soluciones automatizadas de parches dado que, rara vez, la aplicación manual de estos es eficaz en relación con su costo.

Usar las experiencias pasadas para guiar las acciones futuras
Las métricas de la Sección 5.1 se pueden utilizar para determinar hasta qué punto está mejorando la gestión de puntos vulnerables. Las organizaciones también pueden utilizar muchos de estos indicadores, como las tasas de fracaso del parche o de éxito del cambio, para calificar el grado de riesgo de los cambios. Por ejemplo, si un tipo de cambio específico ha sido históricamente problemático, el riesgo de implementar futuros parches de ese tipo se puede disminuir aumentando el número de prácticas de prueba de preimplementación.

[14] El concepto de trabajo planificado comparado con trabajo no planificado se analiza minuciosamente en la guía GTAG 2: Controles de Gestión de Parches y Cambios [5].
[15] En el contexto de ITIL, esto puede denominarse como acuerdos de nivel de operaciones.

Esta sección describe las características de las organizaciones de gestión de puntos vulnerables de TI de alto y bajo rendimiento. Estas descripciones y las de la Tabla 4 en la Sección 5.2 servirán de ayuda a las organizaciones para determinar la madurez de la gestión de puntos vulnerables.

4.1 Organizaciones de bajo rendimiento

Como es de esperar, las organizaciones de bajo rendimiento tendrán procesos ineficientes de detección y gestión de puntos vulnerables. Estas organizaciones no detectan las vulnerabilidades con la suficiente frecuencia y no realizan el seguimiento de sus activos de TI. Cuando la organización realiza una detección de vulnerabilidades, la cantidad de cambios ocurridos desde el último escaneo es muy vasta. Por ello, se utiliza una enorme energía para, simplemente, rastrear los nuevos hosts, las aplicaciones y los propietarios de sistemas. Por otro lado, la cantidad de vulnerabilidades detectadas tal vez sea tan grande que la organización se sienta abrumada al abordarlos.

Cada vez que las organizaciones de bajo rendimiento intentan enmendar las vulnerabilidades, sus esfuerzos generalmente no son eficaces y se aborda sólo parte de esas vulnerabilidades. A menudo, esto ocurre porque la organización no ha integrado sus procesos de gestión de puntos vulnerables y de configuración, o en otros casos, porque ni siquiera tienen un proceso de esa naturaleza. Pueden surgir otros problemas a partir de ineficiencias en la gestión de red o en la comunicación entre Seguridad de TI y Gestión de TI, como por ejemplo, que Gestión de TI desoiga las recomendaciones de Seguridad de TI. Además, la organización tal vez confíe en dispositivos de seguridad para proteger computadoras sin parches de seguridad (por ejemplo, servidores proxies, filtros de seguridad y tecnologías de prevención de intrusiones). El software de seguridad no puede reemplazar a un programa sólido de gestión de parches, sino que lo complementa para alcanzar un nivel de seguridad mayor. Finalmente, las redes de las organizaciones de bajo rendimiento, a menudo, están diseñadas como para estar "abiertas", es decir que cualquiera puede conectarse y obtener acceso a toda la red corporativa o de producción.

Las características de las organizaciones de bajo rendimiento, o de aquéllas en sus etapas iniciales de gestión de puntos vulnerables, son fáciles de detectar e incluyen:

Identificación y validación

- La organización escanea los activos de TI que no son de producción, o sólo una pequeña fracción de los activos de TI de producción donde es probable que los riesgos de negocio sean mayores.
- El diagrama de arquitectura de red que muestra la ubicación de los activos de TI y los dispositivos de seguridad perimetral que protegen esos activos está incompleto o es limitado.
- La organización intenta aumentar el alcance del escaneo o supervisión de los activos de TI, pero se lo impide la visibilidad limitada de la red o la resistencia que oponen los propietarios de los activos (por ejemplo, "usted no debe implementar una instrumentación en mis sistemas críticos para la misión").
- Los programas piloto de detección de vulnerabilidades fallan debido a que hay "demasiado ruido", lo que generalmente indica que el entorno de producción desafía los controles (por ejemplo, los administradores o usuarios de TI instalan con frecuencia nuevo hardware y software generando un entorno caótico sin responsabilidades ni posibilidades de seguimiento de proyectos autorizados).
- La organización es incapaz de validar los resultados de los escaneos de vulnerabilidades debido al volumen de datos, la falta de recursos o la falta de pericia técnica para ello.
- Rara vez se realizan escaneos y no hay actividad de seguimiento para asegurar que se han mitigado las vulnerabilidades.
- La organización no tiene un sistema de gestión de activos.
- La organización no tiene registro de la configuración de referencia de sus sistemas, o tiene registros desactualizados y, por lo tanto, no puede medir con facilidad el impacto sobre el sistema de una falla que lo hace vulnerable.
- La organización tiene un alto nivel de variaciones de configuración provocando resultados impredecibles cuando se implementa un parche en todo un grupo de sistemas en el entorno en cuestión.

Evaluación de riesgos y establecimiento de prioridades

- La organización no puede distinguir entre activos de TI críticos y no críticos para, como consecuencia de ello, establecer prioridades entre las acciones de gestión de puntos vulnerables.
- La organización se siente abrumada por la cantidad de vulnerabilidades que debe corregir. La cantidad de vulnerabilidades crece demasiado rápido como para que la organización pueda abordarlas según sea necesario.

Enmiendas

- La organización tiene demasiados sistemas no gestionados y no posee una solución automatizada de parches implementada en forma extensa. Por consiguiente, se les permite a los usuarios reconfigurar sus sistemas según lo deseen.
- El departamento de TI es incapaz de probar adecuadamente los parches para garantizar una implementación exitosa dentro de la organización.
- El programa de gestión de puntos vulnerables genera una cola de trabajo que excede la capacidad de la organización para abordarla. Recuerde, no es suficiente demostrar que existe un riesgo. La organización también debe poder solucionar los problemas sin crear interrupciones en los negocios que sean peores que el riesgo de origen.
- La organización, o bien no tiene programa de gestión de configuración, o tal programa no está integrado con el programa de gestión de puntos vulnerables.
- La organización tiene una gran variación en su configuración de activos de TI y de actividades de operaciones debido a la ausencia de estandarización o de controles de producción ineficaces.

- La organización emplea mucho tiempo en efectuar trabajos no planificados al realizar servicios de mantenimiento en los activos de TI (por ejemplo, colocación de parches en servidores, o ciclos de rupturas o correcciones).

Mejora continua

- La organización tiene unos pocos procesos automatizados para servir de ayuda al esfuerzo de gestión de puntos vulnerables.
- Hay Acuerdos de nivel de operaciones ilógicos, o directamente no los hay, entre Seguridad de TI y Gestión de TI, o entre esta última y los propietarios de negocio de los activos informáticos.
- La organización actúa constantemente en modo reactivo luchando contra los intentos de ataques y contra los ataques exitosos.
- La organización toma conciencia de los incidentes de seguridad sólo por error, por azar o después de haber ocurrido una pérdida.
- La organización no tiene registro de su tasa de parches o de éxito del cambio.

4.2 Organizaciones de alto rendimiento

En contraste, considere el caso de las organizaciones de alto rendimiento que tienen procesos eficaces de gestión de puntos vulnerables. Esas organizaciones tienen las siguientes características:

Identificación y validación

- La organización tiene un sistema eficaz de gestión de activos que mantiene un inventario completo de los propietarios de negocio para todos los activos de TI.
- La organización sabe exactamente qué porcentaje de activos críticos se gestionan por completo.
- La organización realiza escaneos de vulnerabilidades en todos los terceros y socios de negocio, en los clientes de redes privadas virtuales y en cualquier usuario temporal que se conecte a la red.
- La organización puede verificar con exactitud los resultados que devuelven los escaneos de vulnerabilidades e ignora aquéllos que se identifican por error.
- o La organización utiliza prácticas consistentes con las de las organizaciones de alto rendimiento, tal como se describen en la *GTAG 2: Controles de Gestión de Parches y Cambios* [5].

Evaluación de riesgos y establecimiento de prioridades

- La organización evalúa constantemente los riesgos para los activos de TI e implementa los controles de seguridad apropiados para proteger dichos activos.
- La organización puede evaluar el costo de enmienda y, por lo tanto, está mejor preparada para establecer prioridades entre los esfuerzos de enmienda.
- La organización utiliza los datos anteriores de éxitos de cambios y parches a modo de métricas para determinar qué cambios y parches presentan alto riesgo. Al mismo tiempo utiliza un rigor extra cuando se trata de parches de alto riesgo.

Enmiendas

- La organización estandariza las configuraciones de sistemas y reduce significativamente la cantidad de vulnerabilidades singulares en toda la empresa, y por consiguiente, las correcciones singulares.
- La organización sabe exactamente qué grupo debe comprometer para que aborde las vulnerabilidades y proporcione el volumen apropiado de información.
- La organización utiliza una solución automatizada de parches y prueba eficazmente los parches para asegurar la compatibilidad antes de su implementación.
- Si es necesario, la organización crea y ejecuta proyectos de negocio junto con los propietarios de activos para enmendar gran cantidad de vulnerabilidades.
- La organización puede realizar el seguimiento del proceso de enmienda desde su inicio hasta la corrección y validación de resultados.
- La organización puede verificar que los sistemas comprometidos hayan retornado a su estado conocido aceptable.

Mejora continua

Las organizaciones de alto rendimiento tienen procesos eficientes que detectan vulnerabilidades casi en tiempo real, e impulsan configuraciones seguras. Esto se logra a través de lo siguiente:

- Proporcionar recomendaciones de seguridad a la gestión de configuración para desarrollar una próxima generación de sistemas más seguros.
- Aumentar la frecuencia de los escaneos y cobertura.
- Instalar agentes de host que supervisen todas las aplicaciones y ayuden en las actualizaciones de parches y antivirus.
- Exigir que los hosts sean analizados para detectar vulnerabilidades antes de agregarlos a la red o autenticarlos.
- Desarrollar sistemas utilizando guías de configuración segura para minimizar la cantidad de vulnerabilidades que puedan existir.
- Implementar configuraciones estándar de activos de TI para simplificar la implementación de parches.
- Utilizar los éxitos de cambios y parches anteriores a modo de métricas para calificar el grado de riesgo de los parches y determinar si, en efecto, la organización está mejorando su capacidad de mitigar los riesgos de implementación de parches.

Dado que el muestreo de la gestión de puntos vulnerables es muy frecuente, se pueden detectar rápidamente cambios que probablemente indiquen tendencias significativas, como por ejemplo, procedimientos incorrectos de gestión de redes, nuevas clases de vulnerabilidades o grupos de sistemas mal configurados.

Las redes de las organizaciones de alto rendimiento se segmentan apropiadamente a través de toda la organización, teniendo en mente expectativas realistas de que siempre habrá vulnerabilidades en los servicios y en los clientes que operan en la red. Estas organizaciones de alto rendimiento, imponen una variedad de requerimientos de diseño, como por ejemplo, que si se compromete algún sector, este será detectado y puesto en cuarentena en la red local.

Las organizaciones de alto rendimiento tienen un control eficaz de sus redes cuando se dan las siguientes situaciones:

- Pueden identificar todos los activos de TI instalados en la red.
- Tienen un diagrama de arquitectura de red que muestra la ubicación de los activos de TI y de los dispositivos de seguridad perimetral que protegen tales activos.
- Los empleados no tienen permitido reconfigurar sus sistemas de TI arbitrariamente ni instalar software.
- Los escaneos de vulnerabilidades se programan para ejecutarse regularmente, según sea necesario (por ejemplo, en tiempo real, diariamente, mensualmente o trimestralmente).
- Comprometen rápida y eficazmente a los grupos de TI que se necesitan para corregir las vulnerabilidades y, también, a los grupos que tienen la autoridad para implementar parches oportunamente.
- Automatizan los procesos para recoger información sobre vulnerabilidades, comunicar los pasos de las enmiendas junto con los propietarios, implementar tales enmiendas y actualizar el estado de estas.

Las organizaciones de TI de alto rendimiento pueden no ser las más rápidas en implementar parches en respuesta a las vulnerabilidades, pero tienen mejor capacidad para aceptar y ajustarse al trabajo planificado[16]. Tratan los pedidos de Seguridad de TI de la misma manera que lo hacen con cualquier otra necesidad nueva de negocio y están más capacitadas para satisfacer dicho pedido. Estas organizaciones saben que los parches no probados pueden tener un impacto negativo sobre las operaciones y pueden crear mayores riesgos que la vulnerabilidad detectada.

Las organizaciones de TI de alto rendimiento también han establecido Acuerdos de nivel de operaciones formales entre Gestión de TI y los propietarios de negocio que dictan con qué rapidez se deben corregir las vulnerabilidades prioritarias. Además, tienen acuerdos operativos sobre cómo y cuándo se pueden realizar cambios operativos para enmendar las vulnerabilidades.

Los estudios han demostrado que las organizaciones de alto rendimiento sufrirán menos incidentes en comparación con organizaciones de tamaño equivalente[17]. Sus controles preventivos detectan y evitan muchos eventos potencialmente dañinos. Cuando, en efecto, se produce un evento, los controles de detección lo ponen en evidencia de inmediato. Sus controles correctivos y de recuperación responden rápidamente ante un incidente para prevenir o limitar cualquier daño significativo. Las organizaciones de alto rendimiento no se sentirán abrumadas por el flujo constante de detección de nuevas vulnerabilidades, sino que, por el contrario, tendrán un proceso repetible, uniforme y verificable para gestionar y mitigar tales vulnerabilidades.

[16] "Las organizaciones de alto rendimiento tienden a aplicar parches con menos frecuencia que las de bajo rendimiento" [5]

[17] *Estudio de desempeño de los controles de TI: Identificación de controles fundacionales que tienen el mayor impacto en las operaciones de TI, la seguridad y las medidas de desempeño de auditoría*, IT Process Institute, 2006.

5.1 Métricas

Esta sección contiene ejemplos de métricas que se pueden utilizar para medir las prácticas de gestión de puntos vulnerables en una organización. Los diferentes tipos y tamaños de organizaciones probablemente arrojen diferentes resultados en cuanto a métricas. Por lo tanto, el mejor modo de utilizar estas métricas es obteniendo su tendencia a través del tiempo para demostrar las mejoras ocurridas dentro de la organización.

Cuando se utilicen métricas para comparar el desempeño de varias unidades dentro de una organización, aquellas que no utilizan porcentajes o promedios deben convertirse en coeficientes para que los resultados de tales métricas se calculen en función de la cantidad de sistemas de la organización (por ejemplo, cantidad de vulnerabilidades por computadora). En la Tabla 3, se incluye una lista de métricas de ejemplo. Se pueden obtener más ejemplos de métricas en la publicación *Creating a Patch and Vulnerability Management Program* [3] de NIST y en el informe *Report of the Best Practices and Metrics Teams* [7] del Instituto Estadounidense de Contadores Públicos Certificados (AICPA, en inglés).

Métrica	Descripción
Porcentaje del total de sistemas supervisados o escaneados.	Mide cuán completa es la solución de gestión de puntos vulnerables de una organización, si tiene conocimiento de todos o de parte de sus sistemas y si dicha gestión, en efecto, los supervisa.
Cantidad de vulnerabilidades singulares.	Mide la cantidad de variaciones y riesgos [1] que existen entre los sistemas.
Porcentaje del total de sistemas que están sujetos a un proceso de gestión de configuración.	Mide el grado de control de una organización sobre los dispositivos implementados en su red. Por ejemplo, ¿la organización tiene conocimiento de todos los dispositivos nuevos? ¿Cada dispositivo está configurado con los controles de seguridad y gestión de parches apropiados?
Porcentaje de todas las vulnerabilidades detectadas que han sido validadas.	Esta métrica mide el porcentaje de todas las vulnerabilidades que han sido validadas o entre las que se han establecido prioridades. Sirve para destacar la diferencia entre las organizaciones que simplemente recogen datos y aquéllas que actúan en función de esos datos.
Tiempo medio para enmedar una vulnerabilidad.	Mide la eficiencia de una organización en enmedar las vulnerabilidades.
Porcentaje de vulnerabilidades sobre las que se debe actuar y que han sido corregidas en un período predeterminado.	Esta métrica mide la capacidad de la organización para enmendar las vulnerabilidades que merecen ser corregidas. "Vulnerabilidades sobre las que se debe actuar" se refiere a la diferencia que se debe realizar entre el conjunto de vulnerabilidades y sólo aquéllas que deben ser corregidas.
Porcentaje de acuerdos OLA donde se han alcanzado las metas de rendimiento.	Esta métrica mide la eficacia de los acuerdos OLA que la organización ha establecido para sí y para otros grupos.
Porcentaje del tiempo empleado por Seguridad de TI en trabajos no planificados.	Esto es una medida de cuán eficaz es la organización en implementar los cambios de calidad en los activos de TI, y cuál es el menor tiempo empleado en reaccionar ante cambios fallidos o incidentes de seguridad.
Cantidad de incidentes de seguridad.	Mide la cantidad de situaciones en las que se compromete la confidencialidad, integridad o disponibilidad de los activos de TI de una organización.
Impacto de los incidentes de seguridad.	Mide, en el mejor grado posible, las pérdidas totales en dólares debido a incidentes de seguridad. Aquí se incluyen tiempo y costos insumidos en la investigación y corrección del incidente, además del impacto sobre el negocio.

Tabla 3: Métricas de gestión de puntos vulnerables

5.2 Las diez preguntas principales que los DEA deben realizar sobre gestión de puntos vulnerables

En la Tabla 4, se incluyen las 10 preguntas que un DEA debe realizar para determinar la madurez de las prácticas de gestión de puntos vulnerables de la organización. Las respuestas sirven para ilustrar y comparar las que uno podría llegar a escuchar en una organización de tamaño similar.

Pregunta	Organizaciones de bajo rendimiento	Gerente en negación	Organizaciones de alto rendimiento
1) ¿Qué porcentaje del total de sistemas se supervisan o escanean?	No estamos seguros. Hemos comenzado a realizar los escaneos, pero descubrimos nuevas redes todo el tiempo. O: Cero. Tenemos prohíbido realizar escaneos. O: Probablemente un 2%. Aún estamos probando los escáneres de detección de vulnerabilidades.	Sin duda alguna, 100%. Preguntamos a gran cantidad de grupos qué redes utilizan y las hemos escaneado a todas. O: Sólo estamos escaneando el 35% de nuestra empresa. Después de todo, esas son las redes críticas y lo único que debemos escanear.	Creemos que el 100%. Utilizamos una combinación de entrevistas personales y procesos técnicos para descubrir nuevos hosts y auditar todos los hosts conocidos a fin de detectar vulnerabilidades. Usamos agentes hosts, así como escaneos de vulnerabilidades pasivos y activos para detectar lo que podríamos haber omitido. O: 100% y lo podemos verificar. Estamos conectados con la gestión del cambio y podemos determinar eficientemente si estamos escaneando o no la red completa.
2) ¿Cuántas vulnerabilidades singulares existen en su empresa?	Probablemente muchas, no lo hemos analizado. O: Realizamos un escaneo de vulnerabilidades y no detectamos ninguna. O: Ahh... hay muchas. ¿Qué sabemos ahora?	El mes pasado, descubrimos más de 400, pero es díficil decir con certeza porque la red cambia permanentemente. O: Dado que sólo escaneamos unas pocas redes, sólo detectamos 15 vulnerabilidades singulares.	Tenemos menos de 50 vulnerabilidades singulares, pero nuestra red está diseñada considerando que cada servicio tendrá vulnerabilidades. No obstante, compensamos eso con otros factores de mitigación, como por ejemplo, filtros de seguridad, sistemas de red, sistemas de prevención de instrusiones de host y ejecutando nuestras aplicaciones con privilegios mínimos. O: Hay sólo 15 vulnerabilidades singulares en nuestros sistemas de producción, pero existen 45 en nuestras redes corporativas. Sabemos exactamente qué ocasiona la variación y estamos comprometidos a reducir esa cifra a la mitad el próximo trimestre.
3) ¿Qué porcentaje de sistemas están gestionados?[18]	Sólo se gestionan las máquinas de producción. Dejamos que la gente haga lo que desee en la red corporativa.	Todos..., con seguridad. Al menos, todos los importantes.	Actualmente gestionamos el 100% de todos los dispositivos críticos y de producción, y el 80% de todos los otros dispositivos de la red. A fin del trimestre vamos a completar el proyecto de gestionar el 20% de máquinas que quedan, o bien, vamos a retirarlas de la red. O: Se gestiona el 100% de los dispositivos IP. No se conecta nada sin autorización previa y eso implica que TI respalde por completo la máquina en cuestión.

Tabla 4: Las 10 preguntas principales del auditor

Continúa en página 12

[18] El término "gestionado" se refiere a tener una persona exclusiva a cargo, que tenga la responsabilidad de mantener la disponibilidad del hardware y del software del activo de TI.

Pregunta	Organizaciones de bajo rendimiento	Gerente en negación	Organizaciones de alto rendimiento
4) ¿Qué porcentaje de vulnerabilidades ha validado?	Hay tantas que, en este momento, sólo podemos verificar aproximadamente el 10%.	Empleamos un personal de tiempo completo que valida todas las vulnerabilidades.	Aproximadamente el 85% Hemos establecido prioridades para aproximadamente el 40% de las vulnerabilidades en función de su gravedad crítica en tres de nuestras aplicaciones más utilizadas y en nuestras dos plataformas más comunes. Hemos validado el 45% restante.
5) ¿Cuál es el tiempo medio para enmendar una vulnerabilidad?	Disculpe, no realizamos ese rastreo. O: Nos lleva aproximadamente dos semanas corregir el material más crítico en producción y alrededor de un mes, toda otra corrección en otros lugares.	Todo se corrige rápidamente. Sabemos que esto es así porque no hemos sabido de ningún incidente de seguridad.	Nuestras vulnerabilidades más críticas se corrigen en el día, lo cual coincide con nuestro acuerdo OLA.
6) ¿Qué porcentaje de vulnerabilidades sobre las que se puede actuar se enemendó en el último trimestre?	No realizamos seguimiento de eso, sólo efectuamos escaneos. Enviamos nuestros resultados de escaneo a los propietarios de negocio y corresponde a ellos determinar el grado de riesgo. O: Obtenemos todo tipo de resultados de los escáneres, pero aún estamos tratando de validar esos resultados.	Siempre implica un costo alto enmendar las vulnerabilidades, de modo que confíamos en filtros de seguridad, y en sistemas de prevención y detección de intrusiones. O: Exigimos que todas las vulnerabilidades reciban el parche adecuado.	Hemos establecido prioridades entre las vulnerabilidades y las agrupamos en cinco categorías: El 100% de nuestras dos categorías de vulnerabilidades principales fueron corregidas y tenemos el compromiso de parte de TI y de los propietarios de activos que, para el próximo trimestre, se corregirá el 100% de las vulnerabilidades de las dos categorías que siguen.
7) ¿Qué porcentaje de acuerdos OLA se cumple?	Hasta el momento, no hemos establecido acuerdos OLA.	Todos los grupos tienen el compromiso de abordar las vulnerabilidades de inmediato. Este es un proceso eficaz que nos ha funcionado durante muchos años y no veo la necesidad de cambiarlo.	Siempre estamos cumpliendo con los acuerdos OLA referidos a las vulnerabilidades más críticas. En los que son menos severos, funcionamos bastante bien, pero la realidad es que los procesos de negocio a veces nos impide cumplir con todos
8) ¿Qué porcentaje del trabajo de Seguridad de TI no es planificado?	Pareciera que todo. Permanentemente estamos reaccionando ante las interrupciones y reparando los sistemas cuyo parche o actualización ha fallado.	Oh, no muy alto realmente. Tenemos algunos "incendios" aquí y allá, pero por lo general, siempre tenemos las cosas bajo control.	Sólo un pequeño porcentaje de nuestro trabajo de Seguridad de TI es no planificado. Dados nuestros procedimientos de gestión del cambio y parches probados eficazmente, así como nuestros controles de seguridad en capas, rara vez nos vemos obligados a reaccionar ante interrupciones.
9) ¿Cuántos incidentes de seguridad han sufrido durante el trimestre pasado?	95, no estamos seguros de dónde provienen ni cómo detenerlos. Ayúdennos.	Sólo tuvimos 35 incidentes el trimestre pasado. Afortunadamente, este valor es menor que el del año pasado, por tanto, sé que estamos mejor.	Sólo tuvimos 3 incidentes de seguridad significativos. Pudimos detectarlos y ponerlos en cuarentena rápidamente, y hemos establecido controles para evitar eventos similares en el futuro.
10) ¿Cuál fue el costo promedio de sus últimos 5 incidentes de seguridad?	Realmente no lo sabemos, no lo hemos evaluado.	No es muy alto. Después de todo, seguimos siendo una empresa rentable.	Hemos realizado un análisis de causas raíces en cinco incidentes ocurridos el año pasado y hemos evaluado su costo. Tres ejercieron un impacto en el negocio durante una hora cada uno, y nos costó $X en Equivalente a puesto de tiempo completo (FTE, en inglés) para realizar la investigación, reparación y recuperación.

Tabla 4: Las 10 preguntas principales del auditor

5.3 Unas palabras sobre la gestión de riesgos y puntos vulnerables

La gestión de riesgos ha sido definida como "el proceso de identificar los riesgos, evaluarlos e implementar las medidas para reducirlos a un nivel aceptable" y, por lo general, incluye los siguientes pasos [3, 4 y 6]:

- **Evaluación de activos:** se identifica el valor general que una organización le asigna a un activo.
- **Evaluación de amenazas:** se identifica la probabilidad de que un evento dañino pueda afectar a un activo.
- **Evaluación de vulnerabilidades:** se identifican todas las debilidades de un activo y el grado de gravedad de estas.
- **Determinación del riesgo:** se evalúan y priorizan los riesgos a los que se expone un activo.
- **Decisión en cuanto al riesgo:** se decide si se acepta, se transfiere o se mitiga el riesgo al que se expone un activo.

El lector observará que muchas de las tareas de gestión de riesgos coinciden con las de gestión de puntos vulnerables. Los autores aceptan que otros tendrán diferentes perspectivas y definiciones para la terminología utilizada en esta publicación, y reconocen que tales diferencias son útiles y saludables. En el contexto de este documento, consideramos la gestión de puntos vulnerables como un esfuerzo táctico de corto plazo que puede llevar días o semanas, mientras que la gestión de riesgos es generalmente un proceso más complejo y estratégico que puede insumir meses. Por último, ciertamente, las metas son similares en cuanto a que ambos procesos reducen la posibilidad de que ocurran eventos dañinos y mejoran la postura de seguridad general de la organización.

5.4 Recursos del auditor interno para combatir las vulnerabilidades

A continuación, se incluye una lista de recursos para los auditores internos como ayuda para comprender los riesgos y la probabilidad de impacto que las vulnerabilidades pueden implicar para la organización.

Sistema de Calificación de Vulnerabilidades Comunes (CVSS, en inglés)[19]: El CVSS es un enfoque abierto para calificar las vulnerabilidades informáticas. Proporciona a los usuarios un método para estandarizar el grado de gravedad de las vulnerabilidades entre proveedores dispares y los ayuda a establecer prioridades entre ellas en función del riesgo que impliquen para la organización. Obtenga más información en www.first.org/cvss.

ISO/IEC 17799: Esta norma se compone de una serie de mejores prácticas de la industria que sirve de ayuda para garantizar que una organización emplee y gestione los controles de seguridad apropiados. Puede obtener más información en www.iso.org.

Las Leyes sobre vulnerabilidades [9]: Este informe describe las Leyes sobre vulnerabilidades, que son seis axiomas acerca de la conducta de las vulnerabilidades y fueron recopilados de un proyecto de investigación continuo a largo plazo.

Base de datos nacional de vulnerabilidades (NVD, en inglés): La NVD es una base de datos amplia de vulnerabilidades de ciberseguridad que reúne todos los recursos referentes a vulnerabilidades gubernamentales de EE. UU. disponibles para el público y proporciona referencias sobre recursos de la industria. Se basa y está sincronizada con la norma de denominación de vulnerabilidades, Exposiciones y vulnerabilidades comunes (CVE, en inglés)[20], y proporciona una calificación del grado de gravedad mediante el uso del sistema CVSS. Obtenga más información en http://nvd.nist.gov.

SANS Top 20: El documento titulado *"Twenty Most Critical Internet Security Vulnerabilities"* es un documento vivo e incluye instrucciones paso a paso e indicadores hacia información adicional útil para corregir esas vulnerabilidades de la seguridad. Esta lista incluye secciones para vulnerabilidades de redes de contacto, Windows, Cross-Platform y UNIX, y se puede obtener en www.sans.org/top20/.

Escáneres de vulnerabilidades: En la Tabla 5 más abajo, se incluyen ejemplos de escáneres de vulnerabilidades, comerciales y de fuente abierta, para aplicaciones y redes.

Escáneres de red	Escáneres de aplicaciones (Web)
nCircle (www.ncircle.com)	AppScan (www.watchfire.com)
Nessus (www.nessus.org)*	Nikto (www.cirt.net/code/nikto.shtml)*
Tenable (www.tenablesecurity.com)	Spi Dynamics (www.spidynamics.com)
Qualys (www.qualys.com)	

Tabla 5: Escáneres de vulnerabilidades

* Herramientas de fuente abierta

[19] La identificación CVE es un nombre de identificación estándar de la industria otorgado por la organización Mitre (http://cve.mitre.org/). Es muy común que se establezcan referencias cruzadas entre los informes de vulnerabilidades y las vulnerabilidades con ID de CVE porque las diferentes organizaciones de seguridad pueden describir una vulnerabilidad de manera diferente, pero todas pueden hacer referencia a la misma ID de CVE.

[20] El Sistema de calificación de vulnerabilidades comunes (CVSS, en inglés) intenta solucionar estos sistemas de calificación dispares creando un esquema común que todos los proveedores pueden utilizar para calificar las vulnerabilidades informáticas. El CVSS también intenta establecer prioridades entre las vulnerabilidades en función del riesgo que impliquen para cualquier organización dada. Si desea más información, visite el sitio www.first.org/cvss.

Ejemplo de un informe de escaneo de vulnerabilidades
La Figura 2 muestra un informe de resumen de un escaneo de vulnerabilidades[21]. Esta vista muestra la vulnerabilidad específica que se detectó, la CVE correspondiente y la cantidad de hosts que se ven afectados. Como estas vulnerabilidades se refieren a productos de Microsoft, también se incluye la ID oficial de vulnerabilidad de Microsoft. Finalmente, también se proporciona un nivel de gravedad para cada vulnerabilidad. Observe que cada proveedor de seguridad tendrá su propia escala de calificación de vulnerabilidades[23]. No obstante, esa calificación sirve para comunicarle al auditor un nivel aproximado de gravedad.

Vulnerabilidad	CVE	Hosts	Calificación
MS01-023: Microsoft IIS printer ISAPI Available (Impresora de Microsoft IIS de extensión ISAPI disponible)	CVE-2001-0241	1	31548
MS01-026: Microsoft IIS CGI Filename Decode Error (Error de decodificación de nombre de archivo CGI Microsoft IIS)	CVE-2001-0333	1	31433
MS01-033: Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow (Desbordamiento del búfer de extensión ISAPI de servicios de Index Server de Microsoft)	CVE-2001-0500	1	31151
MS02-056: Microsoft SQL Server User Authentication Remote Buffer Overflow Vulnerability (Vulnerabilidad de desbordamiento de búfer remoto de autenticación de usuario en servidor SQL de Microsoft)	CVE-2002-1123	1	26939
MS03-007: Microsoft Windows ntdll.dll Buffer Overflow Vulnerability - WebDAV (Vulnerabilidad de desbordamiento de búfer en ntdll.dll, Microsoft Windows - WebDAV)	CVE-2003-0109	1	25302
MS03-026: Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability (Vulnerabilidad de sobrecarga de búfer en interfaz DCOM RPC de Microsoft Windows)	CVE-2003-0352	5	24031
MS04-011: Microsoft Windows LSASS Buffer Overrun Vulnerability (Vulnerabilidad de sobrecarga de búfer en LSASS de Microsoft Windows)	CVE-2003-0533	5	20892
MS04-011: Microsoft Windows Private Communications Transport Protocol Buffer Overrun (Sobrecarga de búfer en protocolo de transporte de comunicaciones privadas de Microsoft Windows)	CVE-2003-0719	5	20892
Apple QuickTime Sample-to-Chunk Integer Overflow Vulnerability (Vulnerabilidad de desbordamiento de entero al copiar una tabla de muestra en Apple QuickTime)	CVE-2004-0431	1	20680
MS04-029: Microsoft RPC Runtime Library Remote Denial Of Service And Information (Denegación de servicio e información remoto en la bilioteca de tiempo de ejecución de RPC de Microsoft)	CVE-2004-0569	1	18497
MS05-011: Microsoft Windows Server Message Block Vulnerability (Vulnerabilidad de bloqueo de mensajes de Microsoft Windows Server)	CVE-2005-0045	7	16746
MS05-019: Microsoft Windows IP Validation Vulnerability (Vulnerabilidad de validación de IP en Microsoft Windows)	CVE-2005-0048	7	15741

Figura 2: Informe de escaneo de vulnerabilidades

[21] Este ejemplo de escaneo de vulnerabilidades ha sido proporcionado por nCircle.

5.5 Glosario

Activos de TI: Cualquier aplicación de software o dispositivo de hardware que se utiliza dentro de la organización para respaldar los servicios de negocio de esta.

Elemento de configuración: Se refiere, generalmente, a cualquier dato relacionado o solicitado para un cambio concerniente al activo de software o hardware.

Enmendar (una vulnerabilidad): Se refiere a las acciones de colocar parches, bloquear o, de alguna otra manera, neutralizar una vulnerabilidad. .

Gestión de configuración: Proceso responsable de mantener la información sobre los Elementos de configuración (CI, en inglés) requeridos en los sistemas de información, incluidas sus relaciones. El objetivo primario de Gestión de configuración es proporcionar datos precisos a todos los sistemas de información y a los procesos operativos de TI cuando y donde sea necesario.

Gestión de incidentes: Proceso a cargo de gestionar el ciclo de vida de todos los incidentes de seguridad. El objetivo principal de la gestión de incidentes es restaurar los servicios de TI para los clientes de la manera más rápida posible.

Gestión de liberaciones: La Gestión de liberaciones es el proceso responsable de la planificación, programación y control del movimiento de liberaciones a los entornos de prueba y producción. El objetivo principal de Gestión de liberaciones es asegurar que se proteja la integridad del entorno de producción y que se liberen los componentes correctos. Gestión de liberaciones trabaja estrechamente con Gestión de configuración y Gestión del cambio.

Gestión de puntos vulnerables: Todos los procesos y tecnologías que una organización emplea para identificar, rastrear y enmendar las vulnerabilidades de TI.

Gestión del cambio: La meta del proceso de gestión del cambio es asegurar que se utilicen métodos y procedimientos estandarizados para manejar con rapidez y eficiencia todos los cambios a fin de minimizar el impacto de los incidentes, relacionados con el cambio, sobre la calidad del servicio y, en consecuencia, mejorar las operaciones diarias de la organización.

Incidente de seguridad: Cualquier evento, malicioso o accidental, que se aprovecha de una vulnerabilidad ocasionando pérdida de ganancias, productividad o vida.

IT Infrastructure Library (ITIL): ITIL es un enfoque que describe las mejores prácticas para las organizaciones de servicios de TI de alto rendimiento..Se ha convertido en un modelo de referencia globalmente aceptado para la gestión de TI.

Organizaciones de TI de alto rendimiento: Estas organizaciones saben exactamente qué dispositivos hay, quiénes son sus propietarios y cómo se los gestiona. Tienen implementados procesos automatizados eficaces para identificar nuevas máquinas y sus vulnerabilidades, así como también, procesos formales para enmendar cualquier vulnerabilidad que genere un impacto en el negocio. Todos los activos de estas organizaciones están apropiadamente clasificados y protegidos.

Organizaciones de TI de bajo rendimiento: Estas organizaciones recién están comenzando con su proceso de gestión de vulnerabilidades. Tienen poco conocimiento sobre qué sistemas hay, quiénes son sus propietarios y cómo se gestionan. Tienen implementados sólo algunos procesos para identificar y enmendar las vulnerabilidades. Aún no han comenzado a realizar el seguimiento de su eficacia.

Propietarios de negocio: Se refiere a los responsables de una función de negocio del activo.

Seguridad de TI (gestión de seguridad, gestión de seguridad de la información): Generalmente, se refiere al grupo que efectúa los escaneos de vulnerabilidades y proporciona recomendaciones a TI sobre qué se debe enmendar y cómo debe hacerse.

Sistema gestionado: Un sistema totalmente gestionado es uno en el que el propietario del activo sigue un proceso estricto para la gestión de cambios y de parches. El propietario sabe exactamente cómo se configura el dispositivo, quién está aplicando qué cambios y cuándo se realizan tales cambios.

Vulnerabilidad: Toda debilidad o exposición de un activo de TI que puede conducir a que se comprometa la confidencialidad, integridad o disponibilidad de un activo.

Vulnerabilidades singulares: Se refiere simplemente a las diferentes vulnerabilidades informadas por un escaneo al respecto. Son representativas de la variedad, en cuanto a configuración de sistemas y diversidad de plataformas, dentro del conjunto de activos de TI.

[1] Kevin Behr, Gene Kim, George Spafford, *The Visible Ops Handbook: Starting ITIL In 4 Practical Steps*, IT Process Institute, 2004.

[2] Jennifer Bayuk, Productive Intrusion Detection, *Computer Security Journal*, Volume XVIII, 3-4, 2002, págs. 23 a 33.

[3] Peter Mell, Tiffany Bergeron, David Henning, *Creating a Patch and Vulnerability Management Program*, Special Publication 800-40 v2.0, NIST, 2005.

[4] Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad (editors), *Security Patterns: Integrating Security and Systems Engineering*, Wiley & Sons, 2006.

[5] Jay R. Taylor, Julia Allen, Glenn Hyatt, Gene Kim, *Controles de gestión de parches y cambios: cruciales para el éxito de la organización*, The IIA, 2005.

[6] Gary Stoneburner, Alice Goguen, and Alexis Feringa, *Risk Management Guide for Information Technology Systems*, Special Publication 800-30, NIST 2002.

[7] Grupo de Trabajo de Seguridad de la Información Corporativa, *Report of the Best Practices and Metrics Teams*, Instituto Estadounidense de Contadores Públicos Certificados (AICPA, en inglés), http://ftp.aicpa.org/CSC/infotech/Security/CISWG2_Final_Report.pdf, 2004.

[8] Oficina de Comercio de Gobierno, IT Infrastructure Library, www.itil.co.uk.

[9] Gerhard Eschelbeck,*The Laws of Vulnerabilities: Which security vulnerabilities really matter?*, Information Security Technical Report, Volumen 10, Edición 4, páginas 213 a 219, http://dx.doi.org/10.1016/j.istr.2005.09.005, 2005.

Sasha Romanosky, CISSP, Ingeniero Eléctrico, título universitario otorgado por la Universidad de Calgary, Canadá. Ha trabajado en el área de tecnologías de seguridad e Internet durante más de 10 años, en especial en los sectores financieros y de comercio electrónico en empresas como Morgan Stanley and eBay. Romanosky es coautor del libro *J2EE Design Patterns Applied and Security Patterns: Integrating Security and Systems Engineering* y ha publicado otros trabajos sobre seguridad de la información. Desarrolló la herramienta FoxTor para la exploración anónima de la Web y es codesarrollador del sistema de calificación de vulnerabilidades comunes (CVSS, en inglés), un enfoque abierto para calificar las vulnerabilidades informáticas. Romanosky, actualmente, está inscripto en la Maestría en Ciencias del Programa de Gestión y Política de Seguridad de la Información en la Escuela de Política y Administración Pública Heinz de la Universidad Carnegie Mellon. Si desea comunicarse con él, envíe un mensaje de correo electrónico a sromanos@cmu.edu.

Gene H. Kim, CISA, es director de tecnología (CTO, en inglés) y fundador de Tripwire Inc. En 1992, cofundó Tripwire mientras estaba en la Universidad de Purdue con el Dr. Gene Spafford. En el año 2004, escribió el libro *Visible Ops Handbook* y cofundó el instituto IT Process Institute, dedicado a la investigación, *benchmarking* y desarrollo de guías prescriptivas para operaciones de TI, seguridad de TI y para los auditores. Kim, en la actualidad, trabaja en la Comisión de Tecnología de Avanzada del IIA. Kim posee un título de Maestría en Ciencias de la Computación de la Universidad de Arizona y título universitario en la misma especialidad de la Universidad de Purdue. Recientemente, Kim fue nombrado uno de los "Top 4 CTOs to Watch" por la revista *InfoWorld* debido a sus "pensamiento de vanguardia y actividades de avanzada". Fue uno de los copresidentes del taller técnico de SANS de abril de 2003, titulado "Auditable Security Controls That Work", fue aclamado por SANS como uno de los cinco obsequios más importantes para la comunidad y una de sus principales iniciativas del año 2003. Kim fue copresidente de la mesa redonda "Best in Class Security and Operations" junto con el Instituto de Ingeniería de Software en octubre de 2003. Posee certificaciones en procesos de auditoría y gestión de TI, además de una certificación de ITIL Foundations. Si desea comunicarse con él, envíe un mensaje de correo electrónico a genek@tripwire.com.

Bridget Kravchenko, CISSP, Gerente de Auditoría de TI de General Motors Corp., responsable del desarrollo y la ejecución de los planes de auditoría de la infraestructura de tecnología, a la vez que respalda los procesos de servicios financieros para apoyar una auditoría integrada. General Motors opera en un entorno de amplia cobertura utilizando numerosos proveedores externos de TI de todo el mundo. Kravchenko tiene más de 10 años de experiencia en servicios de consultoría de TI y posee un certificado de ITIL Foundations. Si desea comunicarse con ella, envíe un mensaje de correo electrónico a bridget.kravchenko@gm.com.

Revisores

La Comisión de Tecnología de Avanzada del IIA, organizaciones afiliadas del IIA, AICPA, el Centro encargado de Seguridad en Internet, el Instituto de Ingeniería de Software de la Universidad de Carnegie Mellon, la Asociación de Seguridad de Sistemas de Información (ISSA, en inglés), IT Process Institute, la Asociación Nacional de Directores Corporativos (NACD, en inglés) y el Instituto SANS participaron en el proceso de revisión. El IIA agradece a las siguientes personas y organizaciones por haber proporcionado sus valiosos comentarios respecto de esta guía.

IAI-Reino Unido e Irlanda

Rohit S. Antao, PricewaterhouseCoopers LLP, EE. UU.

Ken Askelson, JCPenney, EE. UU.

Christine Bellino, Jefferson Wells, EE. UU.

Larry Brown, The Options Clearing Corp., EE. UU.

Alfred Dahlmann, WestLB AG, Alemania

David T. Flynn, Horn Murdock Cole, EE. UU.

Nelson Gibbs, Deloitte & Touche, LLP, EE. UU.

Michael S. Hines, Universidad de Purdue, EE. UU.

Dwayne Melancon, Tripwire, Inc., EE. UU.

Fernando Nikitin, Inter American Development Bank, EE. UU.

Jay Schulman, KPMG, LLP, EE. UU.

Jay R Taylor, General Motors Corp., EE. UU.

Hajime Yoshitake, Nihon Unisys, Ltd., Japón

GTAG

Gestión y auditoría de puntos vulnerables de tecnología de la información

"La gestión de puntos vulnerables es un conjunto de procesos, respaldados por la tecnología, que una organización emplea para identificar, evaluar y mitigar los riesgos de negocio que surgen a partir de la implementación y el uso de procesos y activos de TI. Esta guía fue desarrollada para ayudar a los directores ejecutivos de auditoría a evaluar la eficacia de los procesos de gestión de puntos vulnerables de sus organizaciones. En ella, se recomiendan prácticas específicas para guiar a la organización hacia el logro y sostenimiento de altos niveles de eficacia y eficiencia. Después de leer esta guía, usted tendrá un conocimiento práctico de los procesos de gestión de vulnerabilidades y la capacidad para poder distinguir rápidamente entre una organización de gestión de puntos vulnerables de alto rendimiento y una de bajo rendimiento".

Jay R. Taylor, Director General de Auditoría Global de TI de General Motors Corp.

¿Qué es la GTAG?

Las Guías de Auditoría de Tecnología Global (GTAG) preparadas por el IIA están escritas en un lenguaje directo de negocio para abordar en forma oportuna problemas relacionados con la gestión, el control y la seguridad de la tecnología de la información. La colección GTAG se utiliza como un recurso disponible, para los directores ejecutivos de auditoría, sobre los distintos riesgos asociados a la tecnología y las prácticas recomendadas.

Guía 1: Controles de tecnología de la información

Guía 2: Controles de gestión de parches y cambios: críticos para el éxito de la organización

Guía 3: Auditoría continua: implicancias para el aseguramiento, la supervisión y la evaluación de riesgos

Guía 4: Gestión de la auditoría de TI

Guía 5: Gestión y auditoría de riesgos de privacidad

Consulte la sección de tecnología del sitio Web del IIA en www.theiia.org/technology

The Institute of Internal Auditors

www.theiia.org