

Preparándose para la Auditoría de Seguridad — Recomendaciones para Auditores de TI Principiantes

Identificar riesgos y vulnerabilidades y evaluar la efectividad de las medidas de seguridad perimetral son algunos de los pasos que los auditores de TI principiantes necesitan comprender para realizar revisiones más eficaces de los controles de seguridad.

Por Lakshmana Rao Vemuri, CISA, Consultor Sénior de Seguridad, Paladion Networks

Las organizaciones hacen suposiciones diferentes sobre los niveles de seguridad necesarios para proteger sus sistemas y activos de información. Aunque las empresas puedan diferir en sus ideas acerca de la seguridad de las TI [Tecnologías de la Información], el papel de los auditores internos es el mismo: revisar el entorno de seguridad existente e identificar la efectividad de los controles internos. Desafortunadamente, los auditores de TI noveles se encontrarán con no pocas dificultades. Muchas empresas tienen cortafuegos y sistemas de detección de intrusiones (IDS) mal configurados, carencia de sistemas para detectar no-conformidades con las políticas y procedimientos de TI, usan sistemas antivirus desactualizados y esperan demasiado tiempo para parchear los sistemas cuando se detectan vulnerabilidades. Cada uno de estos temas puede ser un reto para un auditor veterano, por lo que aquéllos que acaban de iniciarse en este campo deberán moverse rápidamente. Además, los auditores noveles necesitan comprender las complejidades de redes informáticas, sistemas operativos, software y hardware a menudo muy dispares. Así, incluso auditores experimentados deben “hacer sus deberes” antes de la auditoría para maximizar el proceso de revisión.

ANTES DE LA AUDITORÍA

Para llevar a cabo con éxito revisiones de controles de seguridad, los auditores de TI principiantes deben aprender con qué contar durante un proceso de auditoría. Adicionalmente, deberían comprender los mecanismos adecuados para identificar riesgos y vulnerabilidades de seguridad, evaluar la efectividad de las medidas de seguridad perimetral y trabajar con la alta dirección de forma eficaz. Las cuestiones fundamentales que un auditor principiante debería tener en mente antes de comenzar una auditoría de seguridad son la determinación de los riesgos y vulnerabilidades existentes, así como el nivel de buen gobierno y conformidad de las TI de la organización.

Una vez que se le ha encomendado a un auditor la tarea de revisar el entorno de seguridad de las TI de una empresa, deberá evaluar los diferentes niveles de seguridad de todos los activos de TI y cómo se protege cada uno de ellos. Se requiere también del auditor dar recomendaciones de cómo mejorar la seguridad de las TI de la organización y certificar si existen controles internos adecuados para asegurar todos los activos de TI. Para hacer las recomendaciones adecuadas y comprender qué controles son necesarios, los auditores deberían identificar las vulnerabilidades y riesgos de seguridad existentes en colaboración con los miembros de la dirección de TI y la alta dirección.

Una forma de identificar riesgos y vulnerabilidades de seguridad antes de la auditoría es recomendando a la organización la realización de una evaluación de riesgos. Aparte de ayudar a los auditores a determinar qué controles serían más efectivos basándose en las necesidades de seguridad de la organización, una evaluación de riesgos puede ayudar a disipar la resistencia a los resultados de la auditoría, permitiendo a la dirección tener una imagen exacta del estado actual de la seguridad antes de tener lugar la auditoría. Si el cliente no ha completado una evaluación de riesgos, el auditor debería realizar una evaluación de riesgos básica para identificar áreas de debilidad, que a su vez ayudará a demostrar la necesidad de un control determinado.

El buen gobierno de las TI se basa en procesos de alta calidad, bien definidos y repetibles, que tienen que estar adecuadamente documentados y comunicados, y requiere la participación y compromiso de la gerencia y de los profesionales de TI y seguridad. Una forma de examinar si una empresa tiene un programa eficaz de buen gobierno de las TI es comprobando que la gerencia ha establecido objetivos, políticas y procedimientos claros y que la gestión de las TI está basada en el uso de marcos de actuación, herramientas o buenas prácticas eficaces. Existen muchos marcos de actuación y buenas prácticas que pueden ayudar a las empresas en su gestión de las TI. Algunos de los modelos más conocidos son la [IT Infrastructure Library](#) de la Office of Government Commerce del Reino Unido, los [Control Objectives for Information and related Technology](#) de ISACA y el [estándar 17799: 2005](#) de la International Organization for Standardization.

Además, al evaluar la eficacia de las prácticas existentes de buen gobierno de las TI, los auditores deberían estar atentos a las siguientes llamadas de atención: ausencia a nivel general de la empresa de controles internos o de un programa formal de gestión del riesgo e ineficacia en los procesos de preparación y publicación de informes financieros de TI. Los auditores de TI deberían fijarse en el nivel de conocimiento de la junta directiva o el comité de auditoría del panorama actual de seguridad de las TI de la organización y si el departamento de TI es incapaz de determinar si la información almacenada en un sistema ha sido alterada o si se ha respetado correctamente su periodo de retención. Aunque estos indicadores no sean los únicos que los auditores internos deberían considerar, representan algunos de los problemas principales que afectan a las organizaciones sin un programa eficaz de buen gobierno de las TI.

IDENTIFICANDO RIESGOS Y VULNERABILIDADES DE SEGURIDAD

En el entorno de seguridad existente, el auditor principiante no debería escatimar esfuerzos en comprender las diferentes amenazas de seguridad que puedan afectar a los activos de TI de la organización. Al examinar el entorno de seguridad, el auditor probablemente se encontrará con uno de los siguientes escenarios:

- Escenario 1: los controles de seguridad de las TI tratan adecuadamente los riesgos y vulnerabilidades de activos de TI. Pueden ser necesarias leves modificaciones para incrementar la eficiencia de los controles existentes.
- Escenario 2: la empresa carece de una verdadera infraestructura de seguridad. Por tanto, como cualquier recomendación será implementada por primera vez, la organización no tendrá la sensación de estar reinventando la rueda o gastando dinero adicional para rehacer controles ya establecidos.
- Escenario 3: el auditor se encuentra con una infraestructura de seguridad actual que no protege adecuadamente los activos de TI debido a una mala configuración, monitorización o gestión. El auditor tiene entonces que identificar los niveles de riesgo actuales, su posible impacto y proporcionar recomendaciones. De esta manera, la organización tiene que emplear tiempo y recursos adicionales para cumplir con las recomendaciones de la auditoría.

Los escenarios 2 y 3 suelen crear las mayores dificultades a los auditores principiantes, debido al nivel de conocimientos necesario para dar recomendaciones de seguridad eficaces. Cuando se encuentra con una empresa que carece de una infraestructura de seguridad adecuadamente establecida (es decir, escenario 2), el auditor puede usar el siguiente plan de acción para explicar el panorama de la seguridad y justificar la inversión en una infraestructura correcta:

- Recomendar la realización de una evaluación de riesgos para determinar el valor de los activos de TI. Esto permitirá a la gerencia comprender las diferentes amenazas de seguridad que pueden afectar o están afectando al negocio.
- Recomendar que el departamento de TI instale herramientas de red pasivas para demostrar la frecuencia de intentos de acceso remoto y sondeos externos. Esto ayudará a los responsables a obtener un conocimiento profundo de la topología de red (es decir, qué servicios están disponi-

bles, qué sistemas operativos están en uso y qué vulnerabilidades pueden estar expuestas en la red).

- Explicar a la alta dirección cómo pueden afectar las amenazas de seguridad a la reputación y estabilidad financiera de la organización.
- Explicar las ramificaciones legales de una brecha de seguridad debida a malos controles internos y las consecuencias de la no conformidad con leyes y regulaciones específicas relativas a datos.
- Proporcionar a los ejecutivos información sobre las últimas estadísticas de *ciberdelitos* y cómo éste ha afectado a organizaciones similares. Esto ayudará a inculcar un sentimiento de urgencia por asegurar los sistemas de TI.
- Hablar con la gerencia acerca de la posibilidad de amenazas internas, enumerando los diferentes activos y sistemas de datos que podrían verse afectados. El auditor podría hacer esto realizando un ejercicio de clasificación de datos e informando a la gerencia de los resultados. Esto ayudará a mostrar cuánto dinero está perdiendo la organización por la ausencia de controles de seguridad apropiados y qué pérdidas de ancho de banda se producen por uso improductivo de recursos de red.

Cuando se auditen organizaciones con una infraestructura de seguridad que no protege los activos de TI adecuadamente (es decir, escenario 3), los auditores pueden recomendar que el departamento de TI:

- Corra una herramienta de escaneo de vulnerabilidades en la red desde fuera de la [zona desmilitarizada](#) (DMZ) del cortafuegos para identificar cualquier vulnerabilidad de seguridad.
- Realice una evaluación de vulnerabilidades de red y remita el informe a la gerencia. El informe debería explicar todas las amenazas de seguridad de las TI y sus impactos, así como exponer cualquier brecha y debilidad de seguridad en la infraestructura de TI.

Si la organización no tiene los conocimientos para realizar un test de vulnerabilidad, debería contratar a un experto o usar herramientas de escaneo para detectar cualquier vulnerabilidad del sistema. En cualquier caso, el personal de TI que use dichas herramientas debe tener un profundo conocimiento de cómo usarlas para obtener los mejores resultados.

LO SIGUIENTE — AUDITAR LA IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL

La alta dirección estará más abierta a aceptar recomendaciones de auditoría si los auditores documentan antes la necesidad de la organización de incrementar sus esfuerzos en seguridad de las TI. En cualquier caso, documentar la eficacia de las medidas de seguridad perimetral es también importante para asegurar que las recomendaciones de la auditoría se implementadas adecuadamente. Puesto que muchas organizaciones usan la seguridad perimetral como su línea de defensa principal frente a amenazas externas, los auditores principiantes necesitan familiarizarse con cómo identificar problemas normales durante y después del proceso de implantación de seguridad perimetral.

Según [SANS Institute](#), una organización de formación e investigación, algunos de los problemas más habituales que se encuentran las empresas durante el proceso de implantación de seguridad perimetral son los siguientes:

- La dirección y el personal de TI piensan que, una vez que está instalado un cortafuegos, tienen suficiente seguridad y no hay necesidad de revisiones y controles de seguridad adicionales en la red interna.
- Existen líneas analógicas y *módems* para conectarse a un proveedor de Internet o tener acceso telefónico a sistemas, pasando por alto, por tanto, las medidas de seguridad perimetrales.
- Se permite el paso sin comprobación a través de los puntos de control de seguridad perimetral de servicios de red de sistemas internos.
- Cortafuegos, *hosts* o *routers* aceptan conexiones de múltiples *hosts* de la red interna y de *hosts* de la red DMZ.

- La organización permite la configuración incorrecta de listas de acceso, lo que supone permitir el paso libre a través de la red a servicios desconocidos y peligrosos.
- Los detalles de los *logs* de registro de las actividades de los usuarios no se revisan regularmente o son insuficientes, disminuyendo, por tanto, la eficacia del sistema de monitorización.
- *Hosts* en la DMZ, o aquellos que corren software de cortafuegos, ejecutan servicios innecesarios.
- El personal de soporte utiliza protocolos sin encriptación para gestionar cortafuegos y otros equipos de la DMZ.
- Se permite el establecimiento de túneles encriptados a través del equipamiento perimetral de la organización sin validar totalmente la seguridad del extremo del túnel.
- La empresa usa aplicaciones de red inalámbrica no seguras o no soportadas.

Los auditores noveles que identifiquen cualquiera de las áreas de riesgo mencionadas deberían recomendar a las organizaciones la adquisición de herramientas de seguridad que ayuden a evaluar la fortaleza de la red y a detectar vulnerabilidades y áreas de riesgo de la misma. Algunas de las herramientas disponibles para diversas actividades incluyen software de auditoría basado en máquina, herramientas de análisis de tráfico de red y detección de intrusiones, programas de gestión y mejora de la seguridad y software de auditoría y encriptación basado en red.

TRABAJANDO CON LA ALTA DIRECCIÓN

Además de identificar vulnerabilidades de red o proporcionar orientación en cuanto a seguridad perimetral, los auditores de TI principiantes podrían terminar trabajando con altos directivos para ayudar a maximizar la implementación de las recomendaciones de la auditoría. Como consecuencia, los auditores necesitan estar atentos a cualquier conducta de los directivos que pueda afectar a los esfuerzos de la organización en la seguridad de las TI y, por tanto, a la aceptación de los resultados de la auditoría.

Primeramente, los auditores necesitan asegurarse de que la gerencia entiende la relación entre las necesidades de negocio y la seguridad de las TI. Cuando la gerencia sabe qué riesgos se relacionan con fines y objetivos de negocio específicos, puede empezar a entender dónde son necesarias inversiones. Como la seguridad de las TI tiene que centrarse en mitigar riesgos del negocio, los auditores tienen que ayudar a la dirección a establecer esta conexión. Otros comportamientos que deben vigilarse incluyen:

- No comprender la importancia de la seguridad de las TI o no ser capaz de cuantificar el valor de la reputación de la organización si tiene lugar una brecha de seguridad.
- Confiar en soluciones temporales o a corto plazo, que conducen al resurgimiento de problemas anteriores.
- Hacer depender la seguridad perimetral únicamente del cortafuegos de un proveedor.
- No gestionar eficaz y eficientemente los aspectos operativos de la seguridad de las TI.
- No comprender las consecuencias de una mala seguridad de la información.
- Asignar a funciones específicas a personas incompetentes o que no pueden desempeñar sus tareas eficazmente, así como no formar adecuadamente al personal de seguridad de las TI.

Cuando se encuentran con cualquiera de los puntos mencionados, los auditores podrían recomendar que la gerencia apoye la implantación de las siguientes buenas prácticas para asegurar la creación de una infraestructura de seguridad más eficaz:

- Conseguir el apoyo de la alta dirección para las iniciativas de seguridad de las TI y asegurar que la gerencia entiende las necesidades de seguridad del negocio y los procesos necesarios para cubrir dichas necesidades.
- Reservar todos los años un fondo para contingencias, con el fin de financiar cualquier problema imprevisto en la infraestructura de seguridad. El proceso de gestión del riesgo debería ser utilizado todo lo posible para identificar qué necesita ser tratado a través del proceso presupuestario normal.

- Diseñar, establecer y hacer cumplir una política de seguridad escrita que sea adoptada en toda la empresa y que enumere procedimientos claros para apoyar los objetivos de seguridad de las TI de la organización.
- Impartir formación frecuente y obligatoria a todos los empleados relativa a la concienciación en seguridad.
- Definir las funciones y responsabilidades del personal clave de seguridad.
- Desarrollar un sistema de gestión de controles de seguridad de las TI y crear sistemas de medida para medir y reportar la efectividad de dichos controles a la gerencia.
- Diseñar una planificación a corto y medio plazo detallando cómo implementar mejoras en la infraestructura de seguridad.
- Adquirir las herramientas de auditoría de seguridad basadas en red necesarias para mejorar el rendimiento de los controles internos.
- Contratar un equipo especializado, con probados conocimientos de seguridad de las TI, o asegurar que los empleados de seguridad son lo suficientemente expertos para asumir las funciones y responsabilidades asignadas.

Tener en mente estos puntos ayudará a los auditores principiantes a trabajar con la gerencia de una forma más productiva y cooperativa, romper cualquier estereotipo que impida la implementación de controles de seguridad y ayudar a las organizaciones a estar encaminadas hacia un entorno de TI más seguro.

SEGURIDAD TI — MÁS QUE USAR HARDWARE Y SOFTWARE

Examinar los esfuerzos en seguridad de una empresa es un componente importante del proceso de auditoría de las TI. Saber qué hacer antes de la auditoría, identificar riesgos y vulnerabilidades de seguridad, auditar medidas de seguridad perimetral y trabajar con la gerencia son todos componentes esenciales de una auditoría de seguridad eficaz. Sin embargo, la seguridad es sólo tan fuerte como el más débil de los eslabones de la organización. Como resultado de ello, el papel de los auditores internos es crucial para asegurar que los activos de TI están protegidos y asegurados adecuadamente. La seguridad de las TI exige, por tanto, más que el uso de hardware y software: las organizaciones deben tener la actitud correcta y establecer el tono adecuado en los niveles más altos para que la seguridad funcione. Sin esta actitud correcta, es más probable que los esfuerzos futuros en seguridad fracasen, y las organizaciones estarán siempre un paso por detrás en sus actividades de seguridad de las TI.

Lakshmana Rao Vemuri, CISA, es consultor sénior de seguridad en Paladion Networks (India). Previamente a su actividad como consultor de seguridad, fue Director de TI de un banco del sector público en la India. Vemuri trabaja en el sector bancario desde hace 23 años y es miembro colegiado del *Indian Institute of Bankers*. También es profesor invitado en el *Institute of Chartered Accountants of India* [Instituto de Censores Jurados de Cuentas de la India] en el Programa de Auditoría de Sistemas de Información. Se le puede contactar en vemuri_rao@yahoo.com.

Originally published in *ITAudit*, Vol. 9, April 10, 2006, published by The Institute of Internal Auditors Inc., www.theiia.org/itaudit.

Translation into Spanish made by www.iso27000.es with the express authorization from the author Lakshmana Rao Vemuri and *ITAudit*.

For any comments on contents or further distribution, please get in contact with *ITAudit*, www.theiia.org/itaudit.

For any comments on the Spanish translation, please get in contact with www.iso27000.es.

Originalmente publicado en *ITAudit*, Vol. 9, 10 de Abril de 2006, publicada por The Institute of Internal Auditors Inc., www.theiia.org/itaudit.

Traducción al español realizada por www.iso27000.es con autorización expresa del autor Lakshmana Rao Vemuri y de la publicación *ITAudit*.

Para cualquier comentario sobre el contenido o su distribución, contacten por favor con *ITAudit*, www.theiia.org/itaudit

Para cualquier comentario sobre la traducción, contacten por favor con www.iso27000.es