Evaluación de las estrategias de seguridad

Breve descripción:

Las estrategias de ciberseguridad implementadas en una organización, deben siempre estar acordes a las necesidades del mercado, por lo que se requiere permanentemente de evaluaciones que permitan tomar decisiones de cambio, actualización o simplemente confirmar la efectividad de la estrategia.

Junio 2023

Tabla de contenido

Introducción

Muchas empresas realizan una auditoría de seguridad al menos una o dos veces al año. Pero también se pueden hacer mensual o trimestralmente. Los distintos departamentos pueden tener distintos calendarios de auditoría, según los sistemas, las aplicaciones y los datos que utilicen. Las auditorías de rutina, ya sean anuales o mensuales, pueden ayudar a identificar anomalías o patrones en un sistema.

Los factores determinantes de la frecuencia con la que una organización elige realizar auditorías de seguridad, dependen de la complejidad de los sistemas utilizados y del tipo y la importancia de los datos en ese sistema. Si los datos en un sistema se consideran esenciales, entonces ese sistema puede auditarse con más frecuencia, pero los sistemas complicados que requieren tiempo para auditarse pueden revisarse con menos frecuencia.

Una organización debe realizar una auditoría de seguridad especial después de:

- Una violación de datos.
- Una actualización del sistema.
- Una migración de datos.
- Cuando se producen cambios en las leyes de cumplimiento.
- Cuando se implementa un nuevo sistema.
- Cuando el negocio crece en más de una cantidad definida de usuarios.

Estas auditorías únicas pueden centrarse en un área específica donde el evento puede haber abierto vulnerabilidades de seguridad. Por ejemplo, si acaba de ocurrir

una violación de datos, una auditoría de los sistemas afectados puede ayudar a determinar qué salió mal.

Someter la infraestructura de TI a una auditoría de seguridad puede ser una tarea desalentadora. Con su arquitectura compleja y cientos de amenazas de seguridad de las que protegerse, necesita una guía completa. Una metodología de auditoría de seguridad de TI consta de pasos a seguir para una evaluación general de la infraestructura de seguridad de la organización, incluidos los aspectos físicos y de "software". Esto ayuda a realizar una auditoría adecuada basada en un marco estándar y siguiendo un proceso simplificado. Desde la recopilación de información hasta el informe final, una metodología de auditoría de seguridad ayuda a hacerlo de manera planificada mediante técnicas de auditorías. Puede ampliar la información a través del siguiente video:

Video 1. Evaluación de las estrategias de seguridad

Enlace de reproducción del video

Video 1. Síntesis del video: Evaluación de las estrategias de seguridad
Las auditorías consisten en evaluar el cumplimiento y si cuentan o no con los mecanismos de seguridad adecuados y tienen las regulaciones pertinentes. La auditoría interna es útil para hacer un balance de la eficacia de su ciberinfraestructura actual o prepararse para una auditoría externa profesional. Las auditorías externas de ciberseguridad, por su parte, se realizan para revisar sistemáticamente la situación actual de su empresa con respecto a la seguridad de sus datos, redes y dispositivos.

1. Técnicas de auditoría

Las pequeñas empresas generalmente no tienen grandes equipos de TI para mantenerse al tanto y monitorear la infraestructura de TI y los problemas de seguridad a diario, lo que significa que es más fácil para los piratas informáticos obtener acceso mientras está ocupado haciendo lo que hace día a día. Si es una pequeña empresa y aún no está trabajando con una empresa de TI externa para sus necesidades de TI diarias, vale la pena contratar una para revisar y auditar la seguridad de TI. Esto lo ayudará a comprender dónde debe tomar medidas para mejorar o disponer del presupuesto para invertir en el monitoreo activo de las áreas que tienen más probabilidades de sufrir violaciones de seguridad.

La frecuencia con la que una organización realiza sus auditorías de seguridad depende de la industria en la que se encuentre, las demandas de su estructura comercial y corporativa, y la cantidad de sistemas y aplicaciones que se deben auditar.

- Las organizaciones que manejan una gran cantidad de datos confidenciales, como servicios financieros y proveedores de atención médica, es probable que realicen auditorías con mayor frecuencia.
- Las organizaciones que manejan solo una o dos aplicaciones les resultará más fácil realizar auditorías de seguridad y es posible que las realicen con menor frecuencia.
- Los factores externos, como los requisitos reglamentarios, también afectan la frecuencia de las auditorías.

1.1. Tipos

Las auditorías de ciberseguridad consisten en evaluar el cumplimiento. Las agencias que realizan una auditoría de seguridad cibernética podrán evaluar si cuentan o no con los mecanismos de seguridad adecuados y, al mismo tiempo, asegurarse de que cumplen con las regulaciones pertinentes.

Las organizaciones que realizan auditorías de seguridad cibernética pueden adoptar "un enfoque proactivo'' al diseñar políticas de seguridad cibernética, lo que da como resultado una gestión de amenazas más dinámica. Las auditorías de ciberseguridad son realizadas por proveedores externos para eliminar cualquier conflicto de intereses. Sin embargo, también pueden ser administrados por un equipo interno, siempre que actúen independientemente de su organización matriz.

El universo de auditoría de ciberseguridad incluye todos los conjuntos de:

- Control.
- Prácticas de gestión y disposiciones de gobierno.
- Riesgo y cumplimiento vigentes a nivel empresarial.

En algunos casos, el universo de auditoría ampliado puede incluir a terceros vinculados por un contrato que contiene derechos de auditoría; con el creciente número de amenazas cibernéticas, se está volviendo fundamental que el plan de auditoría de cada organización incluya la seguridad cibernética. Como resultado, se requiere cada vez más que los auditores auditen los procesos, las políticas y las herramientas de ciberseguridad para garantizar que la empresa cuenta con los controles adecuados. Las vulnerabilidades en la seguridad cibernética pueden plantear

riesgos graves para toda la organización, lo que hace que la necesidad de auditores de ciber y de TI bien versados en auditorías de seguridad cibernética sea mayor que nunca.

Auditoría interna

Una de las trampas comunes para las empresas es asumir que sus soluciones de ciberseguridad se mantienen y administran a través de evaluaciones de riesgo estándar. Este tipo de suposición puede conducir a importantes problemas organizativos. Hoy, de hecho, el desarrollo de tecnologías y su uso en las empresas va mucho más allá del marco de una evaluación general.

En este aparte se cubrirán los pasos para configurar una evaluación de riesgos de seguridad amplia y profunda específica para el negocio.

¿Qué es una auditoría interna y por qué es necesaria?

Una evaluación de ciberseguridad es un paso absolutamente crucial para determinar por qué y cómo la empresa utiliza ciertas tecnologías. Esto le permite establecer objetivos y crear parámetros para los siguientes propósitos:

- **Definición de estándares de seguridad**. La auditoría interna permitirá decidir cuáles son los principios de seguridad y elegir cómo comunicarse sobre el tema con todos los empleados de la organización.
- **Cumplir con las normas y reglamentos**. La auditoría mostrará si las soluciones cibernéticas cumplen con sus propios estándares, pero también con los reglamentos externos obligatorios.
- **Rellenar los vacíos**. Una auditoría en profundidad permitirá identificar los vacíos en sus medidas de seguridad. Podrá realizar las correcciones

necesarias para mejorar su sistema actual e identificar los niveles de rendimiento de sus soluciones implementadas.

La auditoría interna es útil para hacer un balance de la eficacia de la ciber infraestructura actual, o prepararse para una auditoría externa profesional. Durante la primera mitad de 2019, el sitio Forbes.com informó de más de 3.800 infracciones de seguridad que salieron a la luz y resultaron en el compromiso de 4.100 millones de documentos. Además, al realizar al menos una auditoría integral de ciberseguridad cada trimestre, se mantiene al tanto de las últimas tecnologías de ciberseguridad para evitar que esto suceda.

Fundamentos de un plan de auditoría interna de ciberseguridad

La evaluación de los riesgos cibernéticos respalda tanto el análisis de madurez presentado al comité de auditoría y a la junta directiva, como el desarrollo de un plan de auditoría interna de ciberseguridad basado en los riesgos de varios años. El plan plurianual se puede establecer en función de los resultados de la evaluación, realizándose algunas auditorías con más frecuencia que otras, según la urgencia y la naturaleza de otras actividades de evaluación y pruebas realizadas dentro de la organización.

Nota: el plan de auditoría interna de ciberseguridad no está grabado en piedra, puede ajustarse en función de la aparición de nuevos riesgos, los cambios en la intensidad relativa, la importancia de las amenazas actuales y otros cambios organizativos.

El papel de la auditoría interna en el fortalecimiento de la ciberseguridad

La frecuencia y variedad de los riesgos cibernéticos y el daño potencial que pueden causar a las empresas, sus socios comerciales y sus clientes están en constante crecimiento. La mayoría de las empresas se toman en serio estos riesgos, pero se necesitan mayores esfuerzos para abordar los peligros y mantener informados a los líderes empresariales sobre la preparación en ciberseguridad.

Nota: la auditoría interna desempeña un papel crucial en el apoyo a las empresas en la lucha constante por gestionar las amenazas cibernéticas, proporcionando una evaluación independiente de los controles existentes o necesarios, y permitiendo que el comité de auditoría y la junta directiva comprendan mejor y mitiguen los diversos riesgos asociados con el mundo digital.

Autoría externa

Las auditorías externas de ciberseguridad son una excelente manera de revisar sistemáticamente la situación actual de una empresa con respecto a la seguridad de los datos, redes y dispositivos; para averiguar si existen posibles problemas de seguridad y cómo resolverlos antes de que ocurran violaciones de seguridad dañinas.

Las amenazas a la seguridad incluyen prácticas de los empleados, desastres naturales y ataques maliciosos como “malware”, virus y ataques de “phishing”. Asegurarse de contar con medidas de protección y monitoreo resilientes en los correos electrónicos, archivos de datos, monitoreo de red, copias de seguridad de datos y actualizaciones de “software” debería garantizar que la empresa permanezca segura y en línea.

Para guiarlo a través del proceso de revisión del estado de las medidas de seguridad, en este ítem explicamos qué es una auditoría y por qué la empresa necesita una, además de cubrir algunas de las preguntas más frecuentes sobre las auditorías de seguridad.

Nota. Mantener segura la red de TI, incluido el "software", aplicaciones, datos y dispositivos es imprescindible para que el negocio funcione sin problemas y cumpla con las normas. No detectar y resolver posibles lagunas de seguridad puede ser un error costoso que requiere habilidades especializadas para resolver, que la mayoría de personas no tiene en casa. Por esta razón, una auditoría externa de seguridad de TI es algo muy recomendable para que todas las pequeñas empresas consideren dentro del proceso anual de planificación y presupuesto.

¿Cuál es el proceso para una auditoría externa de ciberseguridad?

Ya sea que esté realizando una auditoría internamente o esté solicitando la ayuda de una empresa de TI externa, el proceso de la auditoría de seguridad de TI generalmente seguirá los seis pasos que se describen a continuación; recopilación de datos, definición de la auditoría, definición de las amenazas, evaluación de las medidas de seguridad existentes, priorización y elaboración de una lista de acciones lista para la implementación.

a) **Recopilación de datos, comunicación y discusión.** Sus equipos internos deberán estar abiertos a compartir sus métodos y prácticas para realizar su trabajo con el equipo de TI encargado de realizar su auditoría. A menudo, es mejor nombrar uno o dos portavoces de cada equipo que tengan

experiencia en el trabajo y los procesos del departamento para canalizar la información clave al equipo de auditoría de manera eficiente.

b) **Definición de la auditoría**. El alcance de la auditoría, será necesario compilar una lista de todos los activos que requerirían tiempo y dinero para reparar en caso de una brecha de seguridad. Esto incluirá computadoras y teléfonos móviles, hasta cosas más sutiles, como datos almacenados en sus unidades compartidas, correos electrónicos y carpetas de archivo. Una vez que tenga esta lista, deberá decidir qué activos son los más importantes para su negocio para proteger, y esto formará la base para su auditoría de seguridad.

c) **Definición de sus amenazas.** Usando su lista de activos prioritarios para proteger, enumere las amenazas potenciales para cada uno. Las amenazas pueden ser desde desastres naturales como inundaciones, negligencia de los empleados como contraseñas débiles, traer sus propios dispositivos no seguros al trabajo o dejar una computadora portátil en el tren hasta amenazas externas como piratas informáticos, "malware" y virus.

d) **Evaluar las medidas de seguridad existentes**. Aquí es donde realmente vale la pena usar un equipo externo para evitar cualquier sesgo o pasar por alto áreas clave internamente. ¿Están sus empleados actualizados sobre los últimos métodos de piratería utilizados? ¿A menudo dejan sus dispositivos desbloqueados y muestran datos confidenciales? ¿Se cambian las contraseñas regularmente? Al final de este paso, tendrá una buena idea de qué tan bueno es su negocio para defender sus activos más importantes.

e) **Priorizando**. Una vez que sepa cuáles son sus activos más importantes para proteger y dónde están sus debilidades para protegerlos, puede formar

una lista de prioridades para abordar con su lista de acciones de auditoría de seguridad. Para priorizar su lista de acciones, debe considerar la probabilidad de que se produzca una infracción contra cada activo y equilibrar esto con el daño que sería para su negocio si ocurriera.

f) **Lista de acción**. Ahora se ha hecho el trabajo duro y es hora de que la empresa de TI enumere las formas en que reducirá la amenaza de las brechas de seguridad identificadas. Esto podría ser con nuevo software, capacitación del personal o mejores prácticas para reducir la probabilidad de que se produzcan ataques dañinos o infracciones.

Auditoría interna vs. externa: ¿cuál es la diferencia?

No hay garantía de que la empresa evite un ataque; sin embargo, hacer que un auditor analice las prácticas y herramientas de TI podría ser la diferencia entre que la organización sea la próxima víctima o se mantenga segura. A continuación, se presentan las diferencias entre cada una:

a) Auditorías externas

- Utilizan una amplia gama de herramientas de "software" para encontrar brechas en sus sistemas de seguridad.
- Son profesionales altamente calificados y no son baratos.
- Puede resultar complicado encontrar un profesional que reúna las cualificaciones necesarias.
- Se deben realizar una vez al año.

b) Auditorías internas

- Son menos costosas y más fáciles de administrar.

- Permiten a las empresas recopilar datos y establecer sus propios puntos de referencia en el proceso de auditoría.
- Una auditoría interna puede generar sesgos en el proceso de revisión.
- Muchos comités de auditoría y juntas han establecido expectativas para que la auditoría interna comprenda y evalúe los riesgos potenciales
- Se debe realizar trimestralmente.

¿Cómo realizar una auditoría exhaustiva de ciberseguridad?

Hay varias formas de recopilar los datos necesarios, pero primero tendrá que elegir entre una auditoría interna o externa con conocimiento y amplia experiencia en el tema, donde los auditores externos sean capaces de identificar fallas y brechas de seguridad en la ciberinfraestructura.

La trampa: su alto precio y el hecho de que es difícil identificar profesionales que tengan las habilidades y la experiencia requerida. Sin embargo, el éxito de la auditoría dependerá en gran medida de la capacidad para comunicarse con el auditor. Si el auditor no puede acceder rápidamente a los datos que necesita, la auditoría llevará más tiempo, aumentando innecesariamente la factura y arriesgándose a obtener resultados incorrectos; todos estos factores se combinan para que sea más un lujo que una necesidad, de ahí la propensión de los grandes grupos a considerar la auditoría como un gasto corriente.

Otra posibilidad son las auditorías internas que, para la mayoría de las pequeñas y medianas empresas, son una solución mucho más viable. El jefe de una pyme ya conoce los procesos de la empresa, y puede recopilar los datos que necesita sin alterar

los hábitos de trabajo. Este no es el caso de un auditor externo que primero debe dedicar tiempo a estos puntos antes de poder comenzar la misión.

Cinco preguntas para incluir en la auditoría de ciberseguridad

A pesar de su aparente complejidad y de la idea de que una auditoría interna requiere una enorme cantidad de trabajo, en realidad no es más que definir objetivos e indicadores clave de rendimiento (KPI), y luego verificar la adecuación de las políticas de la empresa con estos objetivos. Las siguientes preguntas arrojan más luz sobre esto.

a. ¿Cuáles son las configuraciones de seguridad?

De acuerdo con algunas prácticas y reglamentos generales de protección de datos, cualquier empresa que trate con ciudadanos de Latinoamérica está legalmente obligada a designar un Oficial de Protección de Datos para supervisar toda la información interna y externa. La persona que designe para esta misión tendrá un papel central que desempeñar en su auditoría: comenzará por determinar qué podría representar un riesgo para el negocio diario. Evidentemente, tendrá que elaborar una lista de los activos:

- Equipamiento informático.
- Información sensible (datos de la empresa y del cliente)
- Cualquier cosa que sea crítica y que lleve tiempo o dinero arreglar en caso de que surja un problema.

Una vez que se hayan identificado los activos, debe decidir sobre el alcance de la configuración de seguridad. Puede dividir aproximadamente los activos en dos grupos:

- Ítems incluidos en la auditoría.

- Elementos que no se incluirán en la auditoría.

Naturalmente, es imposible controlarlo todo. Por lo tanto, debe colocar los activos más importantes en el centro de la auditoría y luego ampliar gradualmente el círculo para determinar qué es realmente esencial.

b. ¿Cuáles son las amenazas que se ciernen?

Una vez que se haya identificado los activos más importantes, se debe identificar qué representa una amenaza para ellos. Este paso es fundamental, porque los problemas que se pueden encontrar son de todo tipo: desde contraseñas insuficientemente protegidas por parte de los empleados y filtraciones de datos, hasta incendios e inundaciones, entre posibles desastres.

La auditoría debe tener en cuenta todas las amenazas, la lista puede ser ilimitada, ya que es imposible protegerse contra todas las amenazas imaginables. Sin embargo, siempre que se priorice lo que es absolutamente crucial para el funcionamiento diario del negocio, esto permite tomar todas las medidas razonables para proteger a los empleados y al negocio de posibles amenazas cibernéticas.

A continuación se presentan los peligros más comunes:

- **Empleados.** La fuerza de una cadena se mide por su eslabón más débil. Si los empleados no son la primera línea de defensa, eso es suficiente para amenazar la integridad de toda su infraestructura. Pregúntese si los empleados están capacitados en ciberseguridad.
- **Suplantación de identidad.** Los ataques de “phishing” son la raíz de la mayoría de las filtraciones de datos. Muchos intentos de “phishing” incluso eluden las medidas de seguridad predeterminadas,

de ahí la importancia de capacitar a los empleados para detectar este tipo de actividad.

- **Amenazas internas**. Nadie quiere imaginar que un colaborador interno pueda perjudicar a su empresa, por pura malicia o por accidente. Infortunadamente, sucede, y es un problema bastante común.
- **Ataques distribuidos de denegación de servicio**. Una falla DDoS esencialmente ataca a un objetivo (generalmente un servidor web), lo sobrecarga y evita que funcione normalmente. Este es particularmente el caso de los sitios comerciales.
- **Contraseñas vulnerables.** La adquisición de contraseñas débiles o la compra ilegal de contraseñas son las técnicas más empleadas por los piratas informáticos para acceder a una red.
- **"Malware".** El "software" malicioso o "malware" puede presentarse de diferentes formas: caballos de Troya, "spyware" y gusanos, sin olvidar el "ransomware" cuya peligrosidad es cada vez más preocupante.
- **Robos y desastres**. Aunque ninguno de estos eventos es probable, las consecuencias financieras de no estar preparado podrían ser graves para la empresa.
- **Equipo de terceros**. Al permitir que los empleados conecten sus dispositivos personales a su wifi o usen unidades USB, se corre el riesgo de debilitar involuntariamente sus protocolos de seguridad.

c. ¿Están funcionando las medidas de seguridad actuales?

Una vez que haya identificado las amenazas que podría enfrentar, deberá hacer un balance para evaluar si las medidas de seguridad actuales están a la altura de la

tarea de defender la ciberinfraestructura. En esta etapa, evaluará todas las medidas de seguridad para identificar debilidades:

- ¿Ciertos procesos de seguridad están desactualizados y deben mejorarse?
- ¿La organización sufre de falta de conocimiento o es negligente en el tema de ciberseguridad?

Esta es un área en la que sería útil recurrir a un auditor externo ya que ningún sesgo interferiría con las conclusiones. La auditoría de seguridad debe abstraerse de sus posibles predisposiciones con respecto a los empleados que ocupan determinadas funciones o incluso del desempeño. Si una persona es más capaz de realizar una función de seguridad cibernética, se le debe asignar esa función para garantizar la protección continua.

d. ¿Cómo clasificar los riesgos?

En la auditoría, la priorización de riesgos es posiblemente el paso más importante de todo el proceso. Primero se debe tomar la lista de amenazas potenciales que discutidas anteriormente, después comparar el daño potencial con la probabilidad de que esas amenazas se materialicen. Luego se asigna una puntuación de riesgo a cada uno. Por tanto, considere un incendio que probablemente destruya su equipo y sus instalaciones. Tal incendio impediría a la empresa continuar con sus actividades por tiempo indefinido. El riesgo puede describirse como “alto”. Dado que un incendio es menos probable que un ataque de “malware”, esta puntuación puede reducirse; al priorizar los riesgos para la evaluación, es importante considerar los siguientes puntos que se presentan a continuación:

- **Tendencias recientes:** ¿Qué métodos utilizan actualmente los piratas informáticos para acceder a los datos? ¿Cuáles son las amenazas cuyo nivel de peligrosidad va en aumento? ¿Hay alguna innovación que proporciona más protección?
- **Tendencias relacionadas con su industria:** si la empresa opera en el sector médico o financiero, es más probable que sea víctima de un intento de violación de su seguridad. ¿Cuáles son las tendencias predominantes en su industria y cómo puede protegerse de ellas de manera más proactiva?
- **Violaciones históricas:** ¿La organización ha sido hackeada alguna vez? ¿Ha habido alguna vez una violación de la seguridad física en el pasado? ¿Tienen medidas para evitar que esto vuelva a suceder?
- **Legislación y cumplimiento:** ¿Es una empresa privada o una organización pública? ¿Quién tiene acceso a estos datos? Por ejemplo, si es una empresa privada y maneja información financiera accesible por un gran número de empleados, el factor de riesgo será alto.

e. ¿Cómo explotar los resultados de la auditoría?

En la última parte, se debe volver a la lista de amenazas priorizadas y decidir cómo proceder con la implementación de medidas de seguridad destinadas a neutralizar o erradicar el riesgo de dichas amenazas. La lista de amenazas puede variar según la empresa, el sector de actividad y el nivel de seguridad requerido.

A continuación, se presentan algunas de las soluciones y medidas de seguridad más comunes para evitar estas amenazas.

- **Talleres de formación.** Incluso las acciones modestas de concientización y capacitación en seguridad pueden contribuir en gran medida a reducir el

impacto de un ataque cibernético. Los empleados son seres humanos, entonces cometerá errores. Sin embargo, la implementación de talleres de capacitación y la organización periódica de sesiones de reactivación de conocimientos, permitirá aumentar la conciencia de los empleados sobre la ciberseguridad y minimizar los errores.

- **Copias de seguridad.** Con el papel cada vez mayor de la tecnología en el lugar de trabajo, muchas empresas ahora están completamente basadas en la nube, por lo que la carga se traslada al almacenamiento y las copias de seguridad en línea. Se estima que casi la mitad de las pequeñas y medianas empresas no tienen un plan de respaldo y recuperación de datos, y el 60 % de esas empresas cierran dentro de los seis meses posteriores a la pérdida de sus datos. Si se realizan copias de seguridad de los datos, con regularidad fuera de la red principal, siempre se tendrá algo a lo que recurrir en caso de crisis.
- **Protección de correo electrónico.** Como se mencionó anteriormente, los ataques de "phishing" van en aumento, en parte debido a su creciente sofisticación y la dificultad para detectarlos. Todo lo que necesita es un clic en un correo electrónico de "phishing" para que el atacante obtenga acceso a sus datos. Es cierto que existen filtros antispam para ayudar a eliminar este tipo de correo electrónico, pero nada supera a los empleados capacitados para reconocerlos.
- **Actualizaciones de "software".** Todos han experimentado este tipo de situaciones: si se enciende la computadora se está instalando y actualizando el "software". Tan molesto como puede ser, también es de suma importancia. Estas actualizaciones de "software" a menudo

contienen los últimos parches de seguridad esenciales para proteger la máquina. Por lo tanto, es muy importante aplicar las actualizaciones manuales del plan de seguridad para que todas las máquinas de la red estén actualizadas.

- **Administrador de contraseñas.** Los seres humanos no están hechos para recordar cientos de contraseñas únicas y complejas. Es por eso por lo que a menudo se usan variaciones de las mismas contraseñas una y otra vez. El "software" de administración de contraseñas guarda contraseñas únicas y complicadas. Permite a los usuarios conectarse fácilmente a un sitio o una aplicación. Esto elimina el riesgo de compartir archivos con las contraseñas y las hace mucho más difíciles de adivinar.
- **Monitoreo de red.** Los ciberdelincuentes no tendrán que esperar una segunda vez para obtener acceso a la red. Para combatir esto, puede valer la pena investigar el mejor "software" de monitoreo de red que pueda alertar sobre actividades sospechosas, como intentos de acceso de fuentes dudosas.

Puntos para recordar: se presentan las herramientas y los conocimientos necesarios para realizar una auditoría de ciberseguridad. No obstante, estos controles internos deben realizarse periódicamente, y no de forma aislada y discontinua. La primera auditoría le permitirá establecer la línea de base para todos los controles futuros, para medir más adelante lo que funcionó y lo que necesita mejorar. Al actualizar continuamente los procesos e invertir en las últimas tecnologías, se está creando una cultura que se enfoca en el impacto de la ciberseguridad y destaca los peligros de no contar con las medidas de seguridad adecuadas.

1.2. Métodos

Las unidades de negocio y los departamentos de tecnología de la información integran la gestión del riesgo cibernético en los procesos de toma de decisiones y las operaciones diarias. Son la primera línea de defensa de una organización. La segunda línea incluye administradores de riesgos de tecnología e información, quienes establecen mecanismos de gobernanza y supervisión, supervisan las operaciones de seguridad e implementan medidas según sea necesario, a menudo bajo el liderazgo del Director de Seguridad de la Información. Cada vez más empresas reconocen la necesidad de una tercera línea de defensa cibernética: una revisión independiente de las medidas de seguridad y su desempeño por parte de la función de auditoría interna.

La auditoría interna debe desempeñar un papel central en la evaluación e identificación de oportunidades para fortalecer la seguridad empresarial. Al mismo tiempo, los profesionales de auditoría interna tienen el deber de informar al comité de auditoría y al directorio que los mecanismos de control a su cargo están establecidos y funcionando adecuadamente, lo cual es una preocupación creciente dentro de los directorios, siendo los directores capaces de hacer frente a las obligaciones legales y financieras.

Método de evaluación del riesgo cibernético y mecanismos de defensa: el examen del riesgo cibernético de una organización comienza con las siguientes preguntas clave:

- ¿Quién puede atacar?

- ¿Tienen la intención de interrumpir el negocio o arruinar la reputación de la empresa?
- ¿Qué tácticas pueden emplear?
- ¿Quieren dinero o propiedad intelectual?
- ¿Qué están buscando y cuáles son los riesgos comerciales que deben mitigarse?
- ¿Podrían sus acciones generar riesgos para la salud y la seguridad?
- ¿Los atacantes son delincuentes, competidores, proveedores independientes, empleados internos descontentos, piratas informáticos motivados por diversos intereses o alguien más?

Las empresas deben establecer un enfoque triple para ayudarse y poder abordar las amenazas identificadas en la revisión de las preguntas mencionadas anteriormente, por ello deben tener en cuenta los siguientes métodos.

a) **Seguridad.** La mayoría de las organizaciones cuentan con mecanismos de control, como defensas perimetrales, gestión de identidades y medidas de protección de datos, para protegerse contra amenazas conocidas y emergentes. Los programas basados en la gestión de riesgos permiten priorizar los controles relacionados con los principales riesgos del negocio.
b) **Vigilancia.** La inteligencia de amenazas, los sistemas de monitoreo de seguridad y los análisis de comportamiento y riesgo ayudan a detectar actividades maliciosas o no autorizadas, como cambios en la configuración de aplicaciones o transferencias de datos inusuales, y ayudan a la organización a adaptarse al entorno cambiante de amenazas cibernéticas.

c) **Resiliencia.** La implantación de protocolos de respuesta a incidentes, herramientas de investigación y planes de continuidad y recuperación del negocio permite rectificar la situación en el menor tiempo posible y reducir el impacto. Permite a una organización segura, vigilante y resiliente establecer las bases para su marco general de evaluación y auditoría interna de seguridad cibernética.

d) **Marco de evaluación de la ciberseguridad.** La auditoría interna también debe aplicar un enfoque global para obtener una visión general del mecanismo de ciberseguridad y evitar dar una falsa sensación de seguridad al realizar solo auditorías específicas como parte de una evaluación de preparación para la seguridad cibernética.

1.3. Características y aplicación

Las auditorías resaltan los puntos débiles, como las puertas traseras que utilizan los ciberdelincuentes para tipos comunes de estafas. El objetivo principal de la auditoría de seguridad es doble:

- Para lograr el cumplimiento con las entidades reguladoras y validar estándares certificables en la industria.
- Proporcionar al personal directivo, clientes y proveedores una evaluación detallada de la postura de seguridad de la empresa.

El propósito principal de cualquier auditoría de seguridad es comprender cuántos datos tiene y cómo están protegidos. Por tanto, ofrece información sobre qué conjuntos de datos son críticos y los protocolos que necesita para protegerlos. Una auditoría de seguridad de la red ayuda a comprender todos los riesgos de

ciberseguridad que amenazan a la empresa. Estas evaluaciones mejoran la destreza del equipo de TI frente a un ciberataque.

Esto se puede lograr con un proceso de evaluación eficaz, como las auditorías de seguridad, que ayuda a determinar amenazas, establecer controles de seguridad y mejorar aún más la seguridad general de la infraestructura y las operaciones comerciales.

Estándares populares de auditoría de seguridad de la información

Abordando la creciente necesidad de sólidos estándares de seguridad de TI, los órganos rectores y los reguladores de todo el mundo han establecido un sólido estándar de seguridad de la información que es un mandato en la región. Si bien algunos de ellos se aplican ampliamente a toda la industria de TI, muchos de los estándares de auditoría de seguridad de la información que se desarrollan son específicos de la industria:

a) **Cumplimiento de ISO.** La Organización Internacional para la Estandarización (ISO) proporciona pautas para las organizaciones que garantizan la seguridad, la confiabilidad y la disponibilidad de la infraestructura de TI. La ISO/IEC 27001, conocida por sus requisitos del sistema de gestión de la seguridad de la información, es una norma internacional muy popular y ampliamente aceptada.
b) **Regla de seguridad de HIPPA.** El cumplimiento de HIPAA que comprende las Reglas de seguridad especifica los requisitos relacionados con los métodos o técnicas que se espera que adopte una organización para proteger la Información de salud personal (PHI) o (ePHI) de los pacientes.

c) **Cumplimiento de PCI DSS.** El estándar de cumplimiento de PCI DSS se aplica a las organizaciones que se ocupan de los datos de la tarjeta de pago del cliente. Este estándar está diseñado para garantizar la protección de los datos de tarjetas de pago que involucran transacciones de pago en línea.

Importancia de la auditoría de ciberseguridad

Una auditoría de seguridad de la información es un proceso de evaluación que ayuda a identificar vulnerabilidades y riesgos de seguridad en la infraestructura de TI de una organización. La exposición al riesgo no solo afecta la seguridad de los sistemas y la infraestructura, sino que también afecta la operación comercial general. La seguridad de la información no se trata solo de la seguridad de TI, sino también de la seguridad de la información/datos. Entonces, esta es la razón por la que se cree firmemente que la auditoría de seguridad de la información es esencial para todas las organizaciones y debe ser una práctica habitual adoptada por las empresas para mantenerse seguras y en cumplimiento.

- **Determina la postura de seguridad actual.** La auditoría de seguridad de la información claramente ayuda a la organización a determinar el estado de seguridad actual. Los resultados de la auditoría de las organizaciones sabrán si su defensa de seguridad es eficaz o no contra las amenazas. Con esto, la organización puede obtener una mejor comprensión de sus prácticas y sistemas de TI internos y externos. Los informes de auditoría comprenden una lista detallada de hallazgos, destacando áreas débiles y ciertas soluciones propuestas. El informe guiará aún más a las empresas para mejorar sus políticas, procedimientos, controles y prácticas de seguridad.

- **Determina la necesidad de cambio en las políticas y estándares.** El proceso de auditoría de la información ayuda a descubrir áreas débiles y lagunas en los sistemas y controles de seguridad. Destaca la eficacia del sistema de seguridad de TI de la organización. Los informes generados a partir de los hallazgos de la auditoría sugerirán si las políticas, los procedimientos y el control de seguridad implementados son adecuados para proteger a la organización. Las soluciones propuestas y los comentarios guiarán a las organizaciones para realizar los cambios necesarios en el sistema, los estándares y las políticas de seguridad.
- **Proteger el sistema y la infraestructura de TI contra ataques**. La auditoría de seguridad de la información es una forma para que las organizaciones evalúen sus sistemas de seguridad e identifiquen fallas en ellos. La evaluación ayuda a identificar vulnerabilidades y descubrir posibles puntos de entrada y fallas de seguridad que los piratas informáticos pueden comprometer para obtener acceso a sistemas y redes. De esta manera, la auditoría ayuda a mantener un control regular sobre la efectividad de las medidas de seguridad que, a su vez, mantienen seguros los datos valiosos.
- **Evalúa la seguridad del flujo de datos.** La auditoría de seguridad de la información no solo controla la seguridad de los sistemas y redes, sino que también garantiza la seguridad de los datos críticos para el negocio. Los datos son hoy en día un activo esencial de cualquier organización. Dado el valor que tiene, proteger los datos es hoy en día la principal prioridad de todas las organizaciones. Dicho esto, la auditoría de seguridad determina el flujo de datos en toda la organización. Además, los resultados o hallazgos obtenidos del informe ayudan a las organizaciones a sentar las bases para

cualquier mejora o aplicación de la seguridad en la red. Esto ayuda a establecer sólidas medidas de seguridad contra ataques y filtraciones de datos.

- **Verifica el cumplimiento**. La mayoría de los organismos reguladores y gubernamentales de todo el mundo han establecido sólidas medidas, requisitos y estándares de seguridad a los que deben adherirse las empresas para protegerse contra las amenazas de seguridad cibernética prevalecientes. Se espera que las organizaciones aseguren el cumplimiento de varios estándares y proporcionen evidencia de estos. Entonces, aquí es cuando la auditoría de seguridad de la información juega un papel clave para ayudar a las organizaciones a cumplir. La realización de auditorías periódicas ayudará a la organización a determinar si cuenta o no con las medidas adecuadas implementadas para lograr el cumplimiento de diversos estándares y certificaciones de seguridad. La auditoría le da a la organización una dirección para implementar medidas y lograr el cumplimiento.
- **Mantiene actualizadas las medidas de seguridad**. Las auditorías de seguridad periódicas determinarán si las medidas actuales están implementadas y son adecuadas para protegerse contra las diversas amenazas de seguridad. La auditoría brinda una imagen realista de cuán efectivas son las medidas de seguridad y si pueden resistir el panorama de amenazas en evolución. De esta manera mantiene las medidas de seguridad de las organizaciones avanzadas y actualizadas.
- **Formular nuevas políticas y procedimientos de seguridad.** Dependiendo del resultado de la auditoría de seguridad de la información, las empresas

pueden trabajar en áreas de mejora para corregir la brecha en los sistemas. Con eso, pueden formular una nueva política y procedimiento de seguridad para abordar el panorama de amenazas en evolución. La auditoría funciona como una guía para que las organizaciones desarrollen estrategias para implementar controles de seguridad y políticas y procedimientos relacionados para garantizar el cumplimiento. En general, ayuda a la organización a tomar una decisión informada sobre la actualización de sus medidas de seguridad.

- **Efectividad de la capacitación y concientización sobre seguridad**. La auditoría de seguridad de la información destaca fallas en sistemas, procesos y personas. Entonces, con eso, destaca la efectividad de los programas regulares de capacitación y concientización sobre seguridad que lleva a cabo la organización. Esto les da a las organizaciones una verificación de la realidad sobre sus esfuerzos para realizar capacitaciones de seguridad periódicas y si necesitan o no mejorar el programa de alguna manera.
- **Gestión de respuesta a incidentes.** Las auditorías de seguridad de la información determinarán la efectividad de la gestión de respuesta a incidentes de una organización. Destaca la falla en el proceso y prepara a la organización para una situación imprevista. Los informes de auditoría también destacarán si la respuesta a incidentes actual es efectiva o no y, si las organizaciones están preparadas para una emergencia como una brecha de seguridad cibernética.
- **Complementa la infraestructura con la seguridad de TI.** Para cualquier organización determinada, su infraestructura y tecnología de TI deben

coincidir con el nivel de seguridad que implementan. Por lo tanto, una auditoría de TI puede ayudar a las organizaciones a comprender las herramientas de seguridad adecuadas para su negocio. La auditoría ayuda a determinar si la empresa necesita soluciones de seguridad centralizadas o "software" específico para abordar diferentes riesgos y amenazas. La auditoría de seguridad de la información realizada por un experto en seguridad brinda un hallazgo detallado de la auditoría con áreas débiles que deben abordarse y soluciones propuestas para mitigar el riesgo y proteger el negocio en general.

¿La organización necesita una auditoría de ciberseguridad?

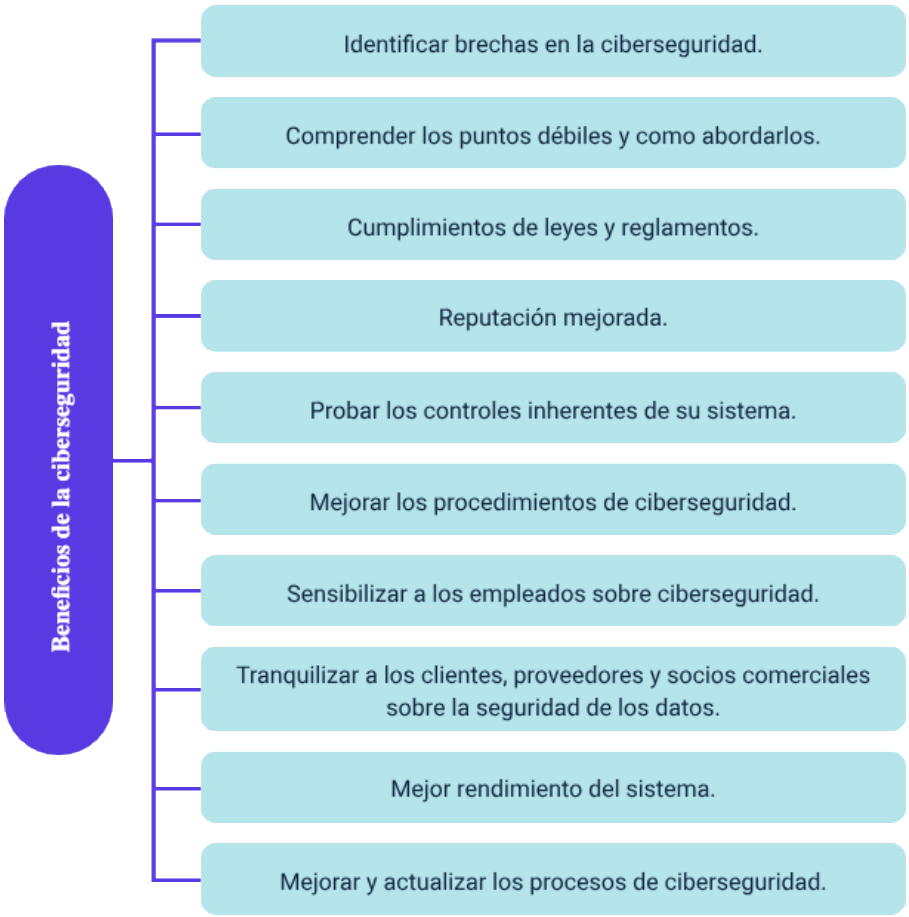
Si una empresa quiere evitar una violación de datos, necesita una auditoría de seguridad cibernética. Estas auditorías ayudan a la empresa a cumplir con los requisitos legales, reglamentarios y contractuales de ciberseguridad.

Una vez que se auditen las prácticas de ciberseguridad de la organización, comprenderá mejor las capacidades de gestión de riesgos. Las auditorías de ciberseguridad también aumentan su reputación como titular de datos. Tienen la oportunidad de aprender sobre la gestión de riesgos y la importancia de la formación de los empleados. También asegura operaciones continuas mientras optimiza los mejores protocolos de gestión de crisis de la organización. Es de recordar que los piratas informáticos apuntan a más que las vulnerabilidades del sistema: también explotan los procesos, procedimientos y empleados de ciberseguridad. Una auditoría de ciberseguridad ofrece una vista panorámica de las debilidades, amenazas y riesgos de ciberseguridad de la empresa, así como el impacto de cada uno.

¿Cuáles son los beneficios de una auditoría de ciberseguridad?

Cuando realiza una auditoría de seguridad cibernética, puede mejorar los sistemas y abordar cualquier debilidad. Estos son algunos de los beneficios más visibles:

Figura 1. Beneficios de la ciberseguridad



Síntesis de la figura: Beneficios de la ciberseguridad
Los beneficios más visibles de la ciberseguridad son: identificar brechas en la ciberseguridad, comprender los puntos débiles y cómo abordarlos, el cumplimiento de leyes y reglamentos, la reputación mejorada, probar los controles inherentes de su

sistema, mejorar los procedimientos de ciberseguridad, sensibilizar a los empleados sobre ciberseguridad, tranquilizar a los clientes, proveedores y socios comerciales sobre la seguridad de los datos, mejorar el rendimiento del sistema y actualizar los procesos de ciberseguridad.

¿Qué cubre una auditoría de ciberseguridad?

Para mantener los datos seguros, es mejor comprender qué cubre una auditoría de seguridad cibernética. El alcance de estas evaluaciones detecta vulnerabilidades y riesgos en toda la infraestructura de TI. Los auditores suelen abordar lo siguiente:

- **Seguridad de datos.** Una auditoría de seguridad de datos comienza con una revisión completa del control de acceso de la red. Los auditores identifican si hay alguna forma de encriptación, la protección en reposo y la transmisión de datos.
- **Seguridad operacional.** Una auditoría de seguridad analiza todas las políticas de seguridad que tiene implementadas. También examina cada procedimiento, proceso y control en la estrategia de prevención de pérdida de datos.
- **Seguridad de la red.** Los auditores revisan todos los controles de red y protocolos de seguridad. Examinan si el centro de operaciones de seguridad está funcionando y verifican si el antivirus está configurado correctamente.
- **Sistema de seguridad.** Los auditores se aseguran de que el proceso de fortalecimiento de los datos funcione correctamente, verifican que los

parches de seguridad estén actualizados y que el acceso privilegiado se administre.

- **Seguridad física.** Los auditores verifican el estado de todos los dispositivos físicos utilizados para acceder a la red. Analizan el cifrado de disco y todos los controles basados en roles.
- **Auditorías internas y externas.** Si se desea realizar una auditoría de seguridad cibernética, el departamento de TI normalmente se puede hacer. Sin embargo, existe una pequeña posibilidad de que no tengan todas las herramientas para realizar dicha tarea correctamente.

La subcontratación puede ser bastante costosa si dirige una pequeña empresa sin departamento de TI. Pero aún puede aprender a auditar la seguridad cibernética de la red. Dicho esto, los auditores externos ofrecen una mirada objetiva e imparcial a los sistemas, identificando hábilmente las debilidades y los problemas. También son los críticos más duros, ya que el análisis imparcial puede descubrir todas las vulnerabilidades de la ciberseguridad. Al final, ofrecerán informes completos con soluciones detalladas para cada problema que encuentren.

Si bien no es la métrica óptima, la elección de auditorías internas o externas finalmente se reduce al presupuesto. La función de auditoría interna en ciberseguridad es analizar y reparar un sistema con el que el equipo de TI está familiarizado. Sin embargo, esto puede generar sesgos o incluso pasar por alto aspectos de la ciberseguridad que tienen el potencial de afectar a la empresa. Los auditores externos, sin embargo, no tienen reparos en dejar saber exactamente dónde se encuentran las debilidades del sistema.

Una auditoría de seguridad cibernética generalmente tiene siete procesos para garantizar el éxito, estos se presentan a continuación:

- **Definir el alcance de la auditoría.** Para una auditoría de seguridad óptima, se enumeran los activos y se agrupan los datos confidenciales. También se necesita conocer el stock de hardware: ¿cuántos dispositivos hay disponibles y operativos? Después del rodeo, se define el perímetro de seguridad para todo. De esa manera, los auditores sabrán qué incluir en el proceso de auditoría y qué dejar de lado.
- **Compartir los recursos con los auditores.** Los auditores necesitan conocer a todos los miembros de los equipos, especialmente a aquellos que trabajan en áreas sensibles. Para realizar una auditoría de ciberseguridad más detallada, el equipo de evaluación debe conocer todos los puntos de contacto con el sistema. Necesitan comprender cómo trabaja cada persona, las herramientas que utilizan y cómo acceden a la red. Así es como los auditores obtienen una mejor comprensión de las políticas de ciberseguridad.
- **Revisar los estándares de cumplimiento.** Antes de pasar por los movimientos de una auditoría de seguridad cibernética, se debe analizar los requisitos de cumplimiento. Estas reglas y regulaciones varían según el estado o país en el que se encuentre. Los auditores necesitan todos los detalles de cumplimiento. Si no se tienen actualizados, ofrecerán un tutorial para garantizar que el negocio se alinee con los requisitos de la industria que realice.

- **Mostrar la estructura de red.** Cuando los dueños de negocios preguntan cuál es el objetivo principal de una auditoría de seguridad, todo se reduce a la divulgación completa de las brechas de seguridad en sus empresas. Los auditores necesitan una visión completa de la estructura de la red. Deben tener acceso al equipo de TI que apoya al equipo de auditoría en cualquier procedimiento para identificar vulnerabilidades. Una vez que encuentran puertas traseras o brechas en su infraestructura, pueden averiguar si está protegido contra ellos o no.
- **Comprender las vulnerabilidades del sistema.** La mayoría de los propietarios de negocios desconocen los riesgos a los que están expuestos antes de realizar una auditoría de seguridad cibernética. Una auditoría es esencialmente una revelación. Puede ver todos los problemas con sus defensas (si los hay). Comprenderá los riesgos que enfrenta en línea y las leyes y regulaciones que se aplican al negocio. También ayuda a que los auditores sepan exactamente qué partes de la red necesitan protección.
- **Evaluar la gestión de riesgos cibernéticos.** Una auditoría de seguridad cibernética ofrece una descripción completa de cada vulnerabilidad en el sistema y cómo los piratas informáticos pueden explotarlas. Esto ayuda a actualizar el plan de gestión de riesgos cibernéticos. Si las políticas de defensa actuales son ineficaces, es hora de una actualización. Se pueden instalar herramientas de análisis mejoradas e implementar una nueva estrategia DLP.
- **Priorizar respuestas.** Una vez finalizada la auditoría de seguridad cibernética, se puede decidir qué hacer a continuación con un mejor sentido de prioridad. La auditoría identifica qué parte de la red está más

expuesta y ofrece soluciones para resolver estos problemas. Al priorizar las amenazas más apremiantes, se asegurará de que los datos de la empresa estén seguros mientras evita la mayoría de los ataques cibernéticos.

Lista de verificación de auditoría de ciberseguridad

Una lista de verificación de auditoría de seguridad cibernética incluye los requisitos básicos que deben evaluar los auditores. La mayoría de los elementos de la lista de verificación se adaptan a cada empresa según la industria y el tamaño del negocio. Sin embargo, en cada auditoría se incluye un conjunto básico de categorías. Estos son los elementos esenciales que debe solicitar independientemente de su nicho:

Tabla 1. Lista de chequeo

ITEM	Sí	No
Un inventario de todos los activos de “hardware”.		
Un inventario de todo el “software” utilizado en la empresa.		
Herramientas para la gestión continua de vulnerabilidades.		
Controles de privilegios administrativos.		
Configuración de seguridad de “hardware” y “software” en todos los dispositivos, como portátiles, terminales, servidores y “smartphone”.		

ITEM	Sí	No
Horarios de mantenimiento y monitoreo, así como registros de auditoría.		
Protección de correo electrónico y navegador.		
Defensas contra “malware”.		
Acceso controlado a los puertos de red, incluidos todos los protocolos y datos del servidor.		

¿Con qué frecuencia se realiza una auditoría de ciberseguridad?

Una vez que aprenda a auditar la seguridad cibernética, debe responder otra pregunta: ¿con qué frecuencia debe ejecutar estas auditorías en los sistemas? La respuesta es engañosa. Depende del tamaño de la empresa y presupuesto. Las grandes multinacionales realizan auditorías de seguridad cibernética mensualmente ya que manejan grandes centros de datos. Una empresa mediana requiere estas auditorías dos veces al año, dependiendo del volumen de las operaciones. Las pequeñas empresas solo necesitan una auditoría anual.

Pensamientos finales

Como propietario de un negocio, se debe comprender los riesgos y amenazas en internet. La red no está exenta de actores maliciosos. Las auditorías de ciberseguridad están diseñadas para ayudar a comprender las vulnerabilidades del sistema. Las auditorías periódicas pueden ayudar a aumentar la seguridad de los datos mientras mejoran la reputación con los clientes y socios comerciales. Una auditoría de

ciberseguridad adecuada se centra en los datos y las operaciones en curso. Destaca las partes débiles de la infraestructura y red. Las auditorías de seguridad ayudan a mejorar la seguridad con informes detallados que indican lo que se debe mejorar. Las auditorías analizan todos sus activos y garantizan que sus procesos de seguridad funcionen de manera eficiente con actualizaciones y rectificaciones recomendadas.

Nota. Las auditorías de seguridad garantizan una auditoría en profundidad de la infraestructura de una organización y sus posturas de seguridad. Ayuda a determinar la exposición al riesgo, detecta vulnerabilidades y fallas de seguridad que pueden afectar la seguridad de la organización. En general, la auditoría de seguridad de la información facilita la gestión de riesgos, el gobierno de riesgos, la continuidad del negocio y la gestión de incidentes, la gestión de riesgos de terceros y el cumplimiento de los mejores estándares y regulaciones de la industria establecidos por los órganos rectores y reguladores mundiales de la industria.

1.4. Técnicas de recopilación de información

Las auditorías de ciberseguridad ayudan a las organizaciones a establecer si sus prácticas, políticas y herramientas de ciberseguridad actuales están a la altura de la tarea de mantener los datos y sistemas seguros. Sin embargo, las auditorías de seguridad cibernética pueden ser difíciles de realizar con regularidad cuando no se está seguro de qué buscar exactamente. Aunque técnicamente no es un requisito para realizar una auditoría de seguridad cibernética, el uso de las herramientas y tecnologías adecuadas facilitará mucho el proceso. Por ejemplo, el uso de una solución de descubrimiento y clasificación de datos le dará una mejor comprensión de qué datos tiene, dónde se encuentran y qué tan confidenciales son los datos. Con este

entendimiento, puede desarrollar una política de seguridad de la información que sea más relevante para los datos.

El uso de una plataforma de seguridad de datos automatizada y en tiempo real le permitirá generar informes personalizados, que se pueden presentar a los auditores para darles una idea de los controles que tiene implementados y cuán efectivos son. Por ejemplo, puede generar un informe que enumera todas las cuentas de usuario (incluidas las cuentas de usuario inactivas) y los privilegios asociados. Una solución de auditoría en tiempo real proporcionará un desglose completo de exactamente quién accede a qué datos, cuándo, desde dónde y desde qué dispositivo.

Recolección de información en ciberseguridad

El marco NICE está diseñado por NIST para proporcionar un vocabulario y definiciones comunes para varios trabajos y conjuntos de habilidades de ciberseguridad. Dentro del marco, se definen varios trabajos diferentes y se describen las tareas asociadas y los conjuntos de habilidades. Una tarea importante dentro de la ciberseguridad es recopilar y analizar datos. En esta sesión del tema sobre ciberseguridad y sus auditorías, se describen algunos de los roles de trabajo que realizan esta tarea dentro del dominio cibernético, los conocimientos y habilidades necesarios para hacerlo y cómo obtener este conjunto de conocimientos y habilidades.

- **Creación de requerimientos de cobranza.** El primer paso en el proceso de recopilación de datos es identificar qué datos deben recopilarse. Lograr esto requiere la capacidad de identificar brechas en los datos recopilados actualmente, determinar qué datos deben recopilarse y saber dónde se pueden encontrar esos datos. Una habilidad importante para lograr este

paso es conocer las posibles fuentes de datos. Por ejemplo, saber qué datos se pueden recopilar de puntos finales, redes, datos de código abierto, bases de datos, etc.

- **Recopilación de datos.** Una vez que se ha definido el esfuerzo de recopilación, el siguiente paso es realizar la recopilación real de los datos. Esta etapa del proceso también requiere el conocimiento de las fuentes de datos, pero se centra en los métodos y herramientas necesarios para realizar la recopilación sin introducir artefactos.
- **Procesamiento.** Los datos recopilados rara vez son perfectos. Antes de realizar cualquier análisis, a menudo es necesario realizar un preprocesamiento. Esto permite que el analista elimine cualquier error o artefacto obvio en los datos, identifique los vacíos de recopilación que deben llenarse y estandarice o transforme los datos en un formato utilizable. En esta etapa del proceso, un analista se beneficiaría de una experiencia en análisis de datos, ya que se necesitan herramientas y técnicas específicas para completarlo.
- **Análisis**. La etapa de análisis del proceso es donde la experiencia en ciencia de datos es más valiosa. En esta etapa, el analista debe estar familiarizado con las herramientas y técnicas estadísticas y de extracción de datos necesarias para convertir los datos sin procesar en inteligencia utilizable que pueda probar o refutar las hipótesis del analista. El analista también debe tener habilidades de programación y secuencias de comandos para realizar esfuerzos de análisis a escala y de manera eficiente.
- **Informes.** Una etapa final e importante en el proceso es la presentación de informes. En esta etapa, el analista desarrolla visualizaciones e informes

que permiten a las partes interesadas comprender los esfuerzos de recopilación y análisis y los resultados y conclusiones extraídos del análisis.

¿Quién recopila la información cibernética?

Dentro del marco NICE, NIST define tres roles de trabajo diferentes que realizan la recopilación de información cibernética: analista de explotación, analista de red objetivo y operador cibernético. Si bien estos trabajos pueden realizar tareas muy diferentes, utilizan muchas de las mismas herramientas, técnicas y procedimientos en la etapa de recopilación de datos del trabajo.

- **Un analista de explotación.** Es un profesional de la ciberseguridad que se enfoca en identificar debilidades y vulnerabilidades potencialmente explotables en una red objetivo. Se centra en la recopilación de datos útiles sobre la red de destino, analizándolos, buscando debilidades y determinando si existe o no un vector de ataque potencial.
- **Un analista de red.** Como objetivo aprovecha la tecnología para recopilar datos y rastrear un objetivo humano. Este tipo de analista utilizará datos de fuente abierta y todo lo que pueda recopilarse de los dispositivos del objetivo, para crear un perfil sobre un individuo y determinar sus patrones habituales, redes y más.
- **Un operador cibernético.** Es similar a un analista de explotación, pero se enfoca en la amplitud en lugar de la profundidad. El objetivo de un operador cibernético es recopilar datos de una variedad de fuentes para encontrar, rastrear y explotar objetivos potenciales. La mayor parte de esta función es la recopilación y el procesamiento de datos.

¿Qué se necesita saber?

Si bien estos son tres trabajos muy diferentes, funcionan de manera similar. Los tres necesitarán algunos conocimientos fundamentales, la capacidad de realizar la recopilación, el procesamiento de datos y la comprensión de las implicaciones legales de su función:

- **Fundamentos:** para desempeñar con eficacia cualquiera de los roles laborales que realizan, es necesario conocer los fundamentos de la informática. Los datos importantes pueden almacenarse en una variedad de medios diferentes, y un analista necesita saber cómo recopilarlos independientemente de la ubicación. Las principales fuentes de datos para un analista de ciberinformación son los puntos finales y la red. Un analista debe estar familiarizado con los principales sistemas operativos (Windows, Linux, Mac, Android e iOS), dónde se pueden almacenar datos útiles en estos dispositivos (sistema de archivos, RAM, etc.) y cómo navegar por estos dispositivos y extraer los datos. Los analistas también deben ser competentes en la recopilación de datos de red. Esto podría incluir configurar dispositivos de monitoreo, analizar los datos recopilados y saber qué buscar (estadísticas, datos ocultos, etc.).
- **Recopilación y procesamiento de datos:** un analista de datos cibernéticos tiene la responsabilidad de realizar de manera efectiva cada paso en el proceso de análisis de datos. Cada uno de estos pasos requiere ciertos conocimientos, destrezas y habilidades.
- **Aspectos legales - leyes:** una consideración importante a lo largo del proceso de recopilación de datos son las leyes y reglamentos en torno a la

recopilación de datos. Un recopilador de datos de seguridad cibernética debe estar familiarizado con todas y cada una de las leyes y regulaciones que limitan qué datos se pueden recopilar, cómo se pueden recopilar y cómo se pueden utilizar.

¿Cómo se empieza?

Como se describió anteriormente, los tres roles laborales utilizan herramientas y técnicas similares para lograr sus objetivos. Un solicitante debe tener una base amplia en las técnicas necesarias, con profundidad en ciertas áreas determinadas por el rol específico. El conocimiento general necesario para todos los roles es una formación en **informática, análisis de datos y ciberseguridad**.

- La informática enseña los fundamentos y las posibles fuentes de datos.
- La ciencia de datos ayuda con el procesamiento y el análisis.
- La ciberseguridad puede ser necesaria para recopilar, comprender y actuar sobre los datos recopilados.

Existen buenos recursos para obtener estos antecedentes, y puede ser una buena idea investigar el examen "Certified Ethical Hacker" (CEH), ya que demuestra que un solicitante tiene los conocimientos de informática y seguridad cibernética para el puesto. Más allá de los antecedentes generales, puede ser conveniente centrarse en ciertas áreas de la función específica que respalda la recopilación de datos.

Por ejemplo, un analista de explotación debe centrarse en comprender las vulnerabilidades de la red y el punto final, un analista de la red objetivo puede centrarse en la inteligencia de código abierto y, un operador cibernético puede especializarse en el reconocimiento.

Las diferentes etapas de recopilación de una auditoría

Para cada fase, se describe el propósito de esa fase y el papel de la gestión de TI:

a) **Etapa de anuncio.** Esta es la etapa durante la cual los auditores anuncian su intención de auditar grupos, características, sistemas, etc. La mayoría de los departamentos de auditoría interna intentan planificar su trabajo por adelantado. Incluso pueden conocer su horario planificado con un año completo de anticipación. No pueden divulgar más detalles que los nombres y fechas preliminares de la auditoría, auditor líder o líder del equipo. Cuanto mayor sea la demora, más suave será el plan. Al igual que cualquier otro equipo de operaciones, las personas, el clima, la tecnología y otros factores comerciales retrasan los cronogramas de revisión.
A veces las auditorías son cíclicas y se tienen que hacer trimestralmente, cada dos años, etc. Estas auditorías son más fáciles de planificar. Se conoce la carga de trabajo asociada y tendrá un plan de dotación de personal para cumplir con los recursos necesarios para la auditoría. Sin embargo, a veces los oyentes aparecen sin previo aviso. Esto suele suceder cuando las cosas no salen según lo planeado.

b) **Carta de compromiso.** Los equipos de auditoría utilizan cartas de compromiso comercial para describir los objetivos específicos de la empresa. Tal vez quieran evaluar el cumplimiento de HIPAA o revisar la efectividad de sus controles de administración de acceso e identidad. Deben definir claramente la intención y el cronograma propuesto para cada fase del compromiso. También es una oportunidad para que el equipo de auditoría se presente a la empresa. Comprender el equipo de auditoría

y el papel de cada uno ayudará a que todo el proyecto funcione sin problemas.

Además de establecer los objetivos de la auditoría, la carta de compromiso comercial describe el alcance de la auditoría. Esto implica determinar qué sistemas se pueden revisar y el período de exploración (rango de fechas para la revisión) y otros detalles.

Nota. La información del alcance suele ser solo una estimación de los auditores, ya que es posible que no tengan el conocimiento específico del sistema, para saber si el alcance es demasiado grande o pequeño para lograr los objetivos establecidos.

c) **Actividad de alcance y brechas auto identificadas.** Durante el ejercicio de alcance, el auditor le dirá qué sistemas planea examinar, el período de análisis, la cantidad de muestras que planea tomar, el tamaño de la muestra, etc. Parte de esta información se basará en la experiencia previa con la organización o sistema. Si un grupo interno lleva varios años realizando la misma auditoría, el alcance inicial puede ser correcto. Sin embargo, si esta es la primera vez que se realiza una auditoría, si la composición del equipo ha cambiado o si el sistema se ha sometido a una revisión, es posible que este no sea el caso.

Su fase de anuncio debe incluir una autoevaluación y un análisis de brechas. La mayoría de los auditores le permitirán proporcionarles información sobre defectos conocidos por adelantado. Si tiene un plan de acción y ha completado un proceso de planificación importante, puede ayudar a mejorar su puntaje de auditoría.

Los auditores están más preocupados por asegurarse de que las cosas se hagan bien que por saber quién recibe el crédito, por detectar brechas y hacer cambios. La fase de alcance es un buen momento para revelar las lagunas en la auto identificación. Algunos auditores prefieren que esto suceda durante las negociaciones del compromiso, así que es importante asegurarse de verificar las expectativas.

d) **Trabajo de campo y pruebas de control.** Aquí es donde se llevará a cabo la mayor parte del trabajo pesado. El auditor primero pedirá que se proporcione información sobre los procesos y procedimientos. Los auditores entrevistarán a los administradores del sistema para ver cómo llevan a cabo sus tareas diarias y luego verificarán la documentación de respaldo.

   Los procedimientos operativos escritos son siempre los mejores. Incluso si se hace lo correcto, si no está documentado, puede esperar que el problema se note durante la auditoría final. Sin documentación escrita, no hay garantía de que el proceso se repite de la misma manera cada vez. Si no se documentan, las transiciones o los desastres de los empleados pueden impedir que los administradores habituales realicen sus funciones y provocar cambios en los procesos.

e) **Pruebas de control.** Una vez que el auditor ha identificado todos los controles, verifica su eficacia. Antes de examinar el sistema, los auditores tratan de determinar si los controles cumplen con los objetivos estratégicos. Revisarán el control y asumirán que se ha implementado correcta y consistentemente. También examinarán los aspectos técnicos del control y los sistemas que se supone que debe proteger. Si existe un

riesgo significativo de violaciones de la política, incluso si se implementan los controles, es posible que no se consideren efectivos y deben revisarse. A veces, esto simplemente significa modificar la documentación escrita del control para reflejar mejor su diseño. A veces tendrá que borrar los comandos y empezar de nuevo.

Nota. Una vez que los auditores han evaluado la efectividad de los controles, los revisan. Aquí es donde se ve que algo está funcionando bien. Aunque los controles pueden considerarse efectivos, es posible que no lo sean en la implementación real. Es posible que el procedimiento se haya realizado incorrectamente o no se haya seguido.

f) **Informes.** Los informes suelen tener dos partes principales:

- **Sección 1: declaración de opinión.** El informe del auditor comienza con una declaración de su opinión sobre la eficacia y eficiencia generales de los controles de la organización. Esto debe ser sucinto si todo va bien y no hay problemas importantes que informar.
- **Sección 2: recomendaciones.** La segunda parte del informe contiene recomendaciones. Los auditores no pueden ser demasiado específicos aquí, ya que esto daría lugar a un conflicto de intereses al revisar los controles. Si lo guían paso a paso sobre cómo arreglar el cheque y luego lo aprueban en la siguiente ronda, sus motivos serán cuestionables. Por lo tanto, dirán qué debe corregirse, pero no cómo.

1.5. Recomendaciones

Las auditorías internas regulares son esenciales para garantizar que la organización cumpla con los estándares de cumplimiento antes de ser evaluada por un auditor externo. Las auditorías internas periódicas son un requisito para algunos marcos de seguridad. El análisis de riesgos debe ser un proceso continuo, en el cual una entidad cubierta revisa regularmente los registros para rastrear el acceso a la e-PHI y detectar incidentes de seguridad, evalúa periódicamente la efectividad de las medidas de seguridad implementadas y reevalúa periódicamente los riesgos potenciales para la e-PHI. Estas auditorías están destinadas a realizar una evaluación precisa y exhaustiva de los riesgos y vulnerabilidades potenciales para la confidencialidad, integridad y disponibilidad de la información de salud electrónica protegida en poder de la organización.

Documentación requerida

La documentación completa es fundamental para demostrarle a un auditor de cumplimiento que la organización está tomando las medidas necesarias para cumplir con los requisitos. Dependiendo de su marco, es posible que deba proporcionar a los auditores pruebas de cumplimiento que se remontan a varios años. Esto podría incluir informes de "firewall", resultados de pruebas de penetración, registros de eventos de seguridad, políticas de la empresa, evaluaciones de riesgos anteriores, lo que sea. Mantener estos sólidos informes bien organizados junto con las listas de verificación y otra documentación hará que la realización de evaluaciones de riesgos de TI regulares y auditorías internas sea mucho más fácil.

a) **Hacer un inventario de los activos existentes**

Al realizar una auditoría de seguridad, el primer paso es hacer un inventario de los activos de la organización. Tener una comprensión clara de lo que está actualmente en uso proporcionará una imagen clara de qué activos deben protegerse, cualquier vulnerabilidad asociada y qué controles tiene la organización para protegerlos. Durante este paso, querrá asegurarse de encontrar y documentar todos los activos de TI de la organización. Un análisis de riesgo adecuado debe cubrir todos los activos relevantes, incluido el "software", los datos regulados, las bases de datos, los servidores, las estaciones de trabajo, los dispositivos de seguridad y los procesos comerciales asociados. Según el tamaño de la organización, es posible que este proceso deba facilitarse con el "software" de gestión de activos de TI (ITAM).

Consejos para la gestión de activos de TI

- Revisar las órdenes de compra, los registros de inventario existentes, los informes de ITAM y las instalaciones para el "hardware" y el "software" existentes.
- Supervisar el uso del "software" y la actividad de internet para identificar los programas de TI en la sombra y los servicios en la nube que se pueden reemplazar con alternativas sancionadas.
- Consultar con la alta gerencia para rastrear cualquier activo que se haya adquirido sin saberlo desde la última verificación de inventario.
- Revisar las políticas de traiga su propio dispositivo (BYOD) de su organización para comprender cómo se utilizan los dispositivos personales dentro de la infraestructura.

b) Identificar las amenazas y vulnerabilidades potenciales para cada activo

La gran mayoría de las organizaciones afirman que almacenan datos confidenciales y regulados solo en ubicaciones seguras. Sin embargo, esta confianza está claramente fuera de lugar, aproximadamente el mismo porcentaje de ellos informó que el personal de TI concedió acceso directo a datos confidenciales y regulados, basándose únicamente en una solicitud del usuario en el último año. No es sorprendente que el 54% de estas organizaciones sufrieran hallazgos de auditoría y multas por incumplimiento. Ahora que se tiene un inventario detallado de los activos existentes, es hora de comprender las amenazas y vulnerabilidades que tienen.

Cada riesgo de seguridad que enfrenta la organización tendrá:

- Un activo para proteger.
- Una amenaza que podría explotar los activos.
- Vulnerabilidades que hacen factible un "exploit".

Comprender cómo la infraestructura existente podría dañarse o explotarse es esencial para mitigar cualquier riesgo potencial. El uso de un marco de seguridad cibernética como el NIST RMF (Marco de Gestión de Riesgos del Instituto Nacional de Estándares y Tecnología) es valioso para garantizar que las evaluaciones y auditorías internas aborden los elementos clave de riesgo que la organización podría enfrentar. El RMF consta de **7 pasos** para ayudar a una organización a seleccionar los controles de seguridad apropiados, estos son los siguientes:

- Preparar a la organización para gestionar los riesgos de seguridad y privacidad.

- Categorizar el sistema y la información procesada, almacenada y transmitida en base a un análisis de impacto.
- Seleccionar el conjunto de controles NIST para proteger el sistema en función de la(s) evaluación(es) de riesgos.
- Implementar los controles y documentar cómo se implementan los controles.
- Evaluar para determinar si los controles están en su lugar, funcionando según lo previsto y produciendo los resultados deseados.
- Autorizar el funcionamiento del sistema (después de una decisión basada en el riesgo de un alto funcionario).
- Monitorear continuamente la implementación del control y los riesgos para el sistema.

Si bien el NIST RMF no indica cómo lograr los pasos recomendados, proporciona una guía valiosa para ayudar a la organización a concentrarse en las consideraciones de seguridad más críticas.

- Beneficios de seguir un marco de ciberseguridad:
- Proporciona una mejor comprensión de los riesgos aceptados y aquellos que serán remediados.
- Mejora el enfoque en las áreas más importantes para la seguridad de la organización.
- Facilita las decisiones de gestión de riesgos de TI.
- Ayuda a una organización a cumplir con los requisitos de cumplimiento de seguridad y privacidad.

¿Qué son las amenazas y vulnerabilidades?

Una vulnerabilidad es una falla que podría ser aprovechada por una amenaza para comprometer un activo. Se puede pensar en una vulnerabilidad como el "por qué" o el "cómo" en una evaluación de riesgos. Una amenaza es cualquier actor que podría explotar una vulnerabilidad para afectar negativamente la confidencialidad, integridad o disponibilidad de un activo. Por ejemplo, la investigación realizada por varios "software" *e* encontró que los empleados que se marcharon fueron responsables del 39 % de los incidentes de robo de propiedad intelectual en 2018. Ese mismo informe señala que el 44 % de los encuestados no saben qué están haciendo sus empleados con los datos confidenciales. Un empleado descontento es una amenaza importante, ya que puede explotar una vulnerabilidad, como el acceso sin restricciones al "hardware" de almacenamiento portátil, para robar información confidencial después de un despido involuntario. Otros ejemplos de amenazas y vulnerabilidades son:

- La falta de políticas, procesos y procedimientos de seguridad hace que la organización sea vulnerable a amenazas internas negligentes.
- La falta de copias de seguridad fuera del sitio hace que la organización sea vulnerable a amenazas físicas como inundaciones e incendios.
- Un punto final móvil en un automóvil desbloqueado es una importante vulnerabilidad de seguridad física, ya que un actor de amenazas podría robarlo fácilmente.

c) Identificar los controles de seguridad existentes y las áreas de mejora

Si se está esperando una auditoría de seguridad cibernética, no hay duda de que la organización ya cuenta con salvaguardas existentes para proteger la confidencialidad,

integridad y disponibilidad de los sistemas e información. La verdadera pregunta es si los controles de seguridad existentes son suficientes para cumplir con los requisitos de cumplimiento. Según el Informe de riesgos de TI de Netwrix de 2018, se debe considerar esto:

- De las organizaciones ignoran la mejor práctica de seguridad de revisar los derechos de acceso a los datos de forma regular.
- Entre las organizaciones que no verifican los derechos de acceso a los datos archivados con regularidad, reportó un compromiso de esos datos durante los últimos 12 meses.
- De las organizaciones tienen un plan de respuesta a incidentes aprobado y se aseguran de que este funcione mediante la realización de pruebas y la capacitación de los empleados.

En este próximo paso, tomará las amenazas y vulnerabilidades descritas en el paso anterior, identificará los controles de seguridad existentes y priorizará cualquier reparación necesaria.

A medida que avanza en este proceso, descubrirá qué riesgos de seguridad se están abordando de manera efectiva y qué capacidades deben agregarse para garantizar que se mitiguen las amenazas pendientes. Su marco de gestión de riesgos y los requisitos de cumplimiento de seguridad dictarán aún más las medidas que debe tomar. Una vulnerabilidad es una falla que podría ser aprovechada por una amenaza para comprometer un activo. Puede pensar en una vulnerabilidad como el "por qué" o el "cómo" en una evaluación de riesgos. Algunos de estos ejemplos son:

- **Robo de datos internos.** "Software" de control de dispositivos y prevención de pérdida de datos (DLP) para monitorear y restringir la exfiltración de datos.
- **"Phishing" e ingeniería social.** Capacitación en concientización sobre seguridad para usuarios, puertas de enlace de seguridad de correo electrónico y salvaguardas administrativas, como políticas, procesos y procedimientos.
- **Navegación por internet de alto riesgo y otras amenazas basadas en la web**. Filtros web y "firewalls" para restringir el tráfico de internet, soluciones de monitoreo de la actividad del usuario para garantizar que los sistemas se utilicen de manera segura y adecuada.
- **Empleados fuera del sitio con acceso remoto a los recursos internos.** Autenticación de múltiples factores basada en riesgos, una VPN con funciones de evaluación de postura y controles para evitar la transferencia de datos a terminales móviles.
- **Herramientas, proveedores o contratistas de terceros con una conexión a nuestros sistemas internos.** Un Acuerdo de Socios Comerciales (BAA) que estipula los requisitos de seguridad de terceros, soluciones de monitoreo para alertar sobre actividades sospechosas, limitando el acceso a activos sensibles tanto como sea posible.
- **Credenciales de usuario comprometidas**. Autenticación multifactorial basada en riesgos, limitando los privilegios de los usuarios tanto como sea posible, monitoreando la actividad de los usuarios.

Cómo priorizar nuevos controles de seguridad

No hay duda de que la evaluación de riesgos encontrará una gran cantidad de vulnerabilidades potenciales, no se podrá mitigar todos los riesgos posibles para la

organización; ahí es donde entra la priorización. Dado que no se puede proteger de manera realista contra todo, se debe estar preparado para demostrar a los auditores de seguridad que se ha tomado todas las medidas razonables necesarias para proteger los datos confidenciales bajo custodia.

Las medidas razonables implican la identificación de riesgos plausibles, la evaluación de la probabilidad e impacto y la garantía de que ha abordado los riesgos de mayor prioridad. Cualquier riesgo que no pueda eliminarse por completo debe documentarse con una razón legítima para la limitación en el plan de seguridad. Una matriz de riesgos es una herramienta útil para priorizar los riesgos; le permite describir los factores de riesgo de la organización, los resultados previstos de la estrategia de seguridad y cómo los controles de seguridad existentes cumplen o no los resultados de la estrategia. En la matriz de riesgos, se describen todas las vulnerabilidades y amenazas potenciales, así como los controles de seguridad disponibles para abordarlas.

La categoría de riesgo de un determinado activo se clasifica en función de:

- La gravedad del impacto en caso de verse comprometida.
- La probabilidad de que el dispositivo se vea comprometido.
- Los controles que están disponibles para mitigar el riesgo.

Nota. Una lista de verificación para prevenir el robo de datos por empleados que se van es necesaria. ¿Le preocupa el daño que podría causar un empleado despedido con el acceso a información corporativa confidencial, contraseñas de cuentas y otros datos confidenciales?

d) Entender lo que busca el auditor

El papel de un auditor de seguridad es ofrecer una perspectiva objetiva de las prácticas de seguridad de la organización. Trabajarán con los ejecutivos internos, gerentes y profesionales de TI para garantizar que la organización sea lo más segura y compatible posible. Lo que busca un auditor de seguridad no debería ser una gran sorpresa. Tener una comprensión clara de los marcos y regulaciones de la organización contribuirá en gran medida a anticipar lo que estarán buscando.

Esto es lo que un auditor externo querrá saber:

- ¿De qué datos sensibles es responsable? (PII, PHI, información de tarjeta de crédito, etc.).
- ¿Qué medidas toma actualmente para proteger los datos confidenciales a lo largo de su ciclo de vida (creación, almacenamiento, uso, archivo y eliminación)?
- ¿Cómo cumplen sus controles de seguridad actuales con los requisitos de seguridad y privacidad de los activos protegidos?

Para mejorar la eficacia de las evaluaciones internas, es importante comunicarse con el auditor por adelantado. Es posible que estén dispuestos a proporcionarle las listas de verificación de evaluación de riesgos y otros documentos que utilizarán como parte del proceso.

e) **Convertir las evaluaciones de riesgos de TI en un proceso continuo**

Las investigaciones de "software" especializadas en la materia arrojaron un promedio en sus investigaciones, aunque el 70% de las empresas ya están realizando evaluaciones de riesgos, la mayoría de ellas no lo hace con regularidad. Cumplir los

estándares de seguridad debe ser una prioridad en toda la organización. Las evaluaciones de riesgos simplemente no son un trato único; identificar y mitigar los riesgos debe ser un proceso continuo para garantizar que la organización esté preparada para abordar nuevas amenazas a medida que surjan.

¿Con qué frecuencia se deben realizar evaluaciones de riesgos de TI?

La mejor práctica recomendada es volver a evaluar los riesgos al menos cada uno o tres años. Esto garantiza que sus controles de seguridad sigan siendo adecuados a medida que cambian sus activos de TI y surgen nuevas amenazas y vulnerabilidades.

Si los líderes empresariales no priorizan la seguridad, cumplir con los estándares de cumplimiento será una batalla cuesta arriba.

- Los empleados siguen el ejemplo de los líderes senior; si la seguridad no es una prioridad para sus jefes, es mucho más probable que tampoco lo sea para ellos.
- Si el departamento de TI se trata como un centro de costos (en lugar de un multiplicador de ingresos/capacidad), las actualizaciones de seguridad críticas no obtendrán el soporte que necesitan para implementar y administrar correctamente.
- Si los requisitos de cumplimiento de seguridad se tratan como una obligación legal y una casilla de verificación, la organización corre el riesgo de quedarse atrás en la mitigación de las últimas vulnerabilidades y amenazas.

Estos profesionales de TI necesitaban la aceptación de los líderes empresariales para obtener el presupuesto y el apoyo que necesitaban para las nuevas medidas de seguridad o el personal. Las evaluaciones de riesgo son una excelente manera de aumentar la aceptación; describirán claramente qué brechas de seguridad tiene la

organización, qué actualizaciones se requieren para abordar esas brechas y el impacto que tendría una brecha en esos activos. Estos datos son fundamentales para justificar los presupuestos de TI, especialmente si la necesidad de las actualizaciones no es evidente de inmediato para el personal que no es de TI.

f) Considere aprovechar los proveedores externos

Dependiendo de las necesidades y los recursos de la organización, es posible que se desee considerar contratar a un proveedor de servicios de seguridad administrados (MSSP) que esté familiarizado con los controles de seguridad requeridos por los marcos y regulaciones de la organización. El principal beneficio de los servicios de TI internos es contar con empleados que comprendan las necesidades únicas de la organización.

Si bien el personal dedicado es muy deseable, no siempre es factible, especialmente para tareas especializadas como auditorías de cumplimiento interno e interpretación de registros de soluciones de administración de eventos e información de seguridad (SIEM). Incluso si la organización ya tiene capacidades internas para ayudar a administrar las operaciones diarias, aprovechar las capacidades y la experiencia de un tercero puede proporcionar beneficios significativos. Las ventajas de terceros:

- Una auditoría de un tercero desinteresado proporcionará opiniones más objetivas que una de una parte interesada interna.
- Los consultores de seguridad de terceros pueden solucionar problemas específicos de manera eficiente, lo que permite que el personal se concentre en sus competencias principales.

- Un auditor de seguridad experimentado puede ayudar a garantizar que la organización implemente una auditoría exitosa.

Independientemente de si usa capacidades internas o externas, al final del día, alguien debe ser responsable de garantizar que la organización tenga las capacidades para cumplir con los requisitos de seguridad; en última instancia, este deber recae en la administración. Los equipos de seguridad de TI son un recurso valioso para implementar controles y mantener activos, pero necesitan el apoyo de la administración para que esto suceda. La subcontratación de la seguridad tampoco elimina la responsabilidad de la administración. Una vez que los controles de seguridad están en el lugar, la gerencia aún debe tomar medidas para garantizar que todo el personal siga las indicaciones del reglamento interno.

g) Asegurarse de que el personal sea consciente de sus responsabilidades de seguridad

Las políticas, los procesos y los procedimientos de seguridad simplemente no son negociables. Cuando están equipados con la capacitación y el soporte adecuados, los empleados son un activo valioso para proteger los datos confidenciales. Si bien el tipo y los detalles de la capacitación pueden variar según el nivel de riesgo de sus funciones, todos los miembros del personal con acceso a los activos de TI necesitan algún tipo de capacitación sobre seguridad. La organización también necesita procesos y procedimientos que dicten las mejores prácticas que debe seguir el personal. **¿Por qué las políticas, los procesos y los procedimientos de seguridad son tan críticos?** Tener personal bien capacitado reduce en gran medida la probabilidad de vulnerabilidades de seguridad, como procedimientos inadecuados de manejo de datos, participar en

actividades informáticas de alto riesgo y caer en trucos de ingeniería social de actores de amenazas maliciosos.

- Los empleados informados no solo cometen muchos menos errores de seguridad, sino que también ayudan a identificar actividades sospechosas para que puedan abordarse antes de que conduzcan a una violación de datos.
- Priorizar la seguridad de esta manera también es esencial para cultivar una cultura de cumplimiento dentro de la empresa.
- Invertir en capacitación regular en seguridad (y adherirse a los requisitos) comunica la importancia del cumplimiento a todos los involucrados.

El liderazgo es responsable de garantizar que el personal se tome en serio sus responsabilidades de seguridad. Debe quedar claro desde el día uno a qué estándares se adhiere la organización, por qué esos estándares son críticos y el papel del personal para garantizar que se cumplan estos estándares.

Las mejores prácticas para proporcionar a los usuarios finales formación en seguridad son:

Asigne a alguien para que sea directamente responsable de garantizar que el personal esté informado sobre sus responsabilidades de seguridad.

- Si la experiencia en seguridad no está disponible internamente, contrate a un consultor de capacitación en concientización sobre seguridad cibernética.

- Asegúrese de que cualquier capacitación en seguridad incluya algún tipo de prueba para identificar las áreas en las que el personal puede necesitar capacitación adicional.
- Proporcione capacitación al personal cada 4 a 6 meses para garantizar que sigan siendo conscientes de sus riesgos y responsabilidades.
- Mantenga una política de comunicación abierta que permita a los empleados hacer preguntas cuando no estén seguros del mejor curso de acción.

Plantilla de política de medios extraíbles:

- Establecer estándares de seguridad de datos para el almacenamiento portátil.
- Definir el uso aceptable de los medios extraíbles.
- Informe a los usuarios sobre sus responsabilidades de seguridad.

Las grandes empresas de auditoría recomiendan que las auditorías de seguridad cibernética definan el tema y el objetivo de la auditoría antes de iniciarla. La organización dice que los límites y las limitaciones a considerar para las auditorías de seguridad cibernética incluyen la empresa frente a una esfera de control privada y, si se debe considerar el uso de dispositivos y aplicaciones que no son de agencias. Otro elemento que puede limitar el alcance de la auditoría es si se centrará en la infraestructura de TI interna frente a la infraestructura externa.

Por regla general, el uso de TI se extiende más allá de la red organizacional interna, como en el uso de viajes, entornos de uso doméstico o la adopción de la nube. Si bien esto puede crear un riesgo de seguridad cibernética adicional, se ha convertido

en una práctica común en la mayoría de las empresas. Eso es especialmente cierto con tantos empleados que continúan trabajando desde casa.

Desde la perspectiva de un auditor, es recomendable adoptar una visión basada en el riesgo y definir los objetivos en consecuencia. Además, los objetivos de la auditoría deben limitarse a un alcance razonable y también deben corresponder a los objetivos de ciberseguridad y protección definidos por la empresa.

2. “Hacking” ético

La piratería ética implica un intento autorizado de obtener acceso no autorizado a un sistema informático, aplicación o datos. Realizar un “hack” ético implica duplicar estrategias y acciones de atacantes malintencionados. Esta práctica ayuda a identificar vulnerabilidades de seguridad que luego pueden resolverse antes de que un atacante malicioso tenga la oportunidad de explotarlas.

¿Qué es un “hacker” ético?

También conocidos como “sombreros blancos”, los “hackers” éticos son expertos en seguridad que realizan estas evaluaciones de seguridad. El trabajo proactivo que realizan ayuda a mejorar la postura de seguridad de una organización. Con la aprobación previa de la organización o del propietario del activo de TI, la misión de la piratería ética es opuesta a la de la piratería maliciosa.

¿Cuáles son los conceptos clave del “hacking” ético?

Los expertos en piratería siguen cuatro conceptos clave de protocolo, a saber:

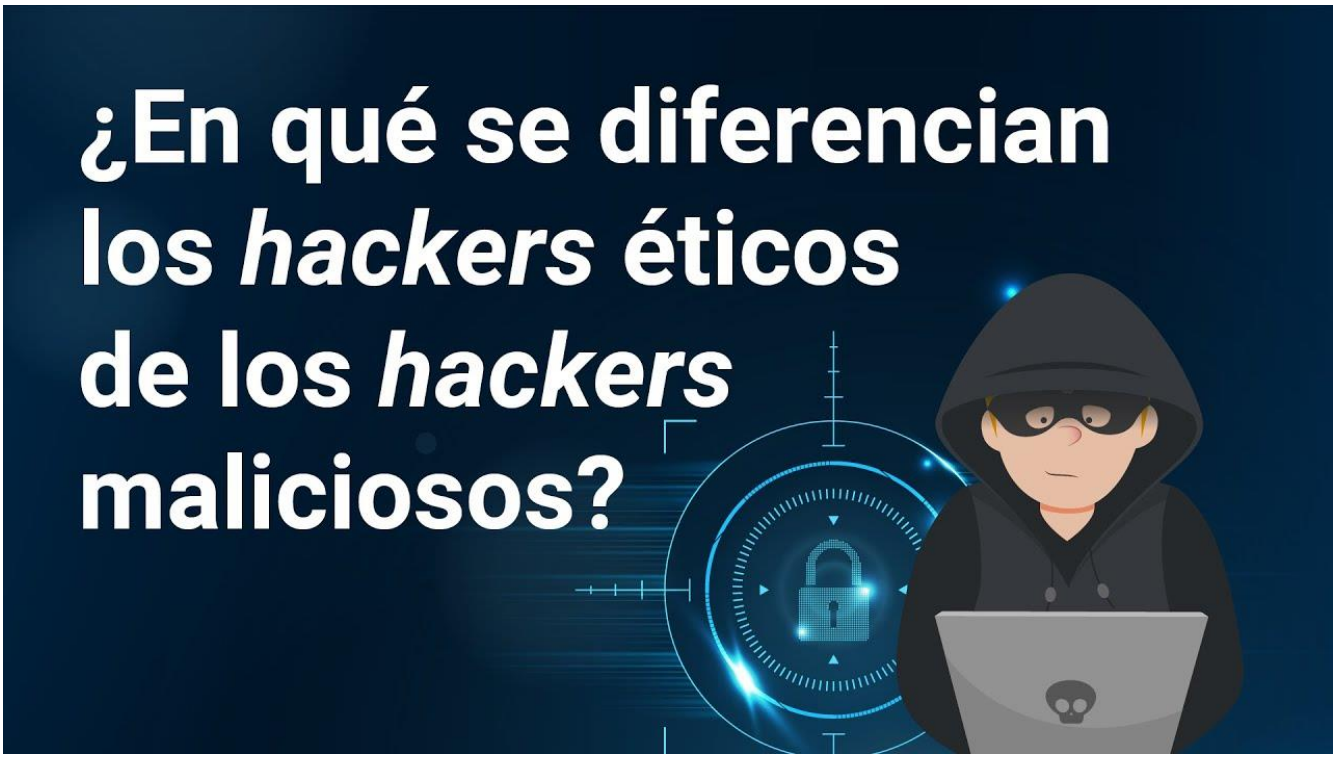
- **Mantenerse legal.** Obtenga la aprobación adecuada antes de acceder y realizar una evaluación de seguridad.
- **Definir el alcance.** Determine el alcance de la evaluación para que el trabajo del “hacker” ético siga siendo legal y dentro de los límites aprobados de la organización.
- **Reportar vulnerabilidades**. Notifique a la organización de todas las vulnerabilidades descubiertas durante la evaluación. Proporcione consejos de remediación para resolver estas vulnerabilidades.

- **Respetar la confidencialidad de los datos.** Dependiendo de la confidencialidad de los datos, los "hackers" éticos pueden tener que aceptar un acuerdo de confidencialidad, además de otros términos y condiciones requeridos por la organización evaluada.

¿En qué se diferencian los hackers éticos de los hackers maliciosos?

Los "hackers" éticos utilizan su conocimiento para asegurar y mejorar la tecnología de las organizaciones. Brindan un servicio esencial al buscar vulnerabilidades que pueden conducir a una brecha de seguridad. En el siguiente video se puede conocer la diferente entre estos dos tipos de "hackers".

Video 2. ¿En qué se diferencia los "hackers" éticos de los "hackers" maliciosos?



Enlace de reproducción del video

Video 2. Síntesis del video: ¿En qué se diferencia los “hackers” éticos de los “hackers” maliciosos?
Un “hacker” ético informa las vulnerabilidades identificadas a la organización. Además, brindan consejos para corregir. En muchos casos, con el consentimiento de la organización, el “hacker” ético realiza una nueva prueba para garantizar que las vulnerabilidades se resuelvan por completo. Los piratas informáticos maliciosos, por su parte, tienen el propósito de obtener acceso no autorizado a un recurso, para obtener ganancias financieras o reconocimiento personal. Algunos piratas informáticos maliciosos desfiguran sitios web o bloquean servidores “back-end” por diversión, daño a la reputación o para causar pérdidas financieras.

¿Qué problemas identifica el “hacking”?

Al evaluar la seguridad de los activos de TI de una organización, la piratería ética tiene como objetivo imitar a un atacante. Al hacerlo, buscan vectores de ataque contra el objetivo. El objetivo inicial es realizar un reconocimiento, obteniendo la mayor cantidad de información posible. Una vez que el “hacker” ético recopila suficiente información, la usa para buscar vulnerabilidades contra el activo. Realizan esta evaluación con una combinación de pruebas automatizadas y manuales. Incluso los sistemas sofisticados pueden tener tecnologías de contramedidas complejas que pueden ser vulnerables. No se detienen en descubrir vulnerabilidades.

Los “hackers” éticos usan “exploit” contra las vulnerabilidades para probar cómo un atacante malintencionado podría explotarlas.

Algunas de las vulnerabilidades más comunes descubiertas por "hackers" éticos incluyen:

- Ataques de inyección.
- Autenticación rota.
- Configuraciones incorrectas de seguridad.
- Uso de componentes con vulnerabilidades conocidas.
- Exposición de datos confidenciales.

Después del período de prueba, los "hackers" éticos preparan un informe detallado. Esta documentación incluye pasos para comprometer las vulnerabilidades descubiertas y pasos para parchearlas o mitigarlas.

¿Cuáles son algunas limitaciones del hacking ético?

- **Alcance limitado**. Los "hackers" éticos no pueden progresar más allá de un alcance definido para que un ataque tenga éxito. Sin embargo, no es descabellado discutir el potencial de ataque fuera del alcance con la organización.
- **Restricciones de recursos**. Los piratas informáticos maliciosos no tienen las limitaciones de tiempo que suelen enfrentar los piratas informáticos éticos. El poder de cómputo y el presupuesto son restricciones adicionales de los "hackers" éticos.
- **Métodos restringidos**. Algunas organizaciones piden a los expertos que eviten los casos de prueba que provocan la caída de los servidores (por ejemplo, ataques de denegación de servicio (DoS)).

2.1. Etapas

El "hacking" ético se ha convertido en un caballero de brillante armadura en el mundo del cibercriminal. Si bien los ataques cibernéticos siguen proliferando en las organizaciones, las industrias y el mundo, la piratería ética brinda a las empresas la solución para ayudarlas a combatir este problema cada vez mayor. Hay diferentes fases del "hacking" ético.

Las condiciones de seguridad de TI son tan graves que, en la mayoría de los casos, las organizaciones tardan hasta 6 meses en darse cuenta de que ha habido una infracción. Es por eso que necesitan trabajar con piratas informáticos éticos para actualizar sus medidas de ciberseguridad y proteger sus datos.

Nota. Las organizaciones necesitan medidas de seguridad de primer nivel para combatir con la gran cantidad de ataques que tienen lugar a diario. Se ha dicho que ocurre un ataque cibernético cada 39 segundos, y los sistemas antiguos no están lo suficientemente equipados para manejarlos a todos. Las actualizaciones periódicas y las actualizaciones de los sistemas de seguridad de TI son la mejor manera de proteger a las empresas contra este problema creciente.

¿Cuáles son las diferentes fases del "hacking" ético?

Las organizaciones emplean "hackers" éticos para simular un ciberataque real en sus sistemas y redes. Este ataque viene en diferentes fases. Se necesita mucha habilidad y esfuerzo para que los piratas informáticos éticos identifiquen todas las vulnerabilidades y las exploten para su máximo beneficio. Este ataque simulado se utiliza para identificar todas las áreas de debilidad que enfrenta la organización para trabajar y fortalecerlas. Las fases del "hacking" ético son:

a) **La fase de reconocimiento.** Esta es la primera etapa en el proceso de piratería ética. El "hacker" de sombrero blanco recopila toda la información disponible sobre las redes y sistemas instalados, así como las medidas de seguridad que se han implementado. El "hacker" ético tiene dos tipos de reconocimiento que puede hacer en esta fase:

- **El reconocimiento activo** busca información sobre el sistema de red, el servidor o la aplicación de destino para aumentar las posibilidades de que se detecte al "hacker" en el sistema. Es mucho más arriesgado que el segundo tipo de reconocimiento, que es el reconocimiento pasivo.
- **El reconocimiento pasivo** es la forma más sigilosa de obtener información sobre el objetivo. Esto se centra en la recopilación de información sobre los miembros clave de la empresa, datos esenciales sobre la empresa, averiguar sus direcciones IP y buscar otros tipos de información crítica. Dado que la mayoría de las organizaciones tienen casi toda su información pública, la recopilación pasiva de información puede ser muy fácil para un "hacker" ético.

b) **La fase de exploración.** La segunda fase en la estrategia de un "hacker" ético es la fase de exploración. Este paso implica utilizar toda la información obtenida en la fase de reconocimiento y aplicarla para buscar vulnerabilidades en el área objetivo. Hay diferentes tipos de escaneos realizados por "hackers" éticos. Pueden buscar puertos abiertos o diferentes servicios que se ejecutan sin protección en la organización.

Los "hackers" éticos también pueden:

- Realizar escaneos de vulnerabilidades para encontrar errores en los servidores de la empresa, que pueden ser explotadas, este proceso se ha automatizado porque hay muchas herramientas disponibles para que los piratas informáticos realicen análisis de vulnerabilidades.
- Crear varios 'mapas' de redes, este proceso de mapeo de red incluye encontrar el "firewall" utilizado por la organización y diferentes enrutadores y redes para ayudarlos durante su proceso de piratería.

c) **La fase de obtención de acceso.** Aquí es donde el "hacker" ético hace el hackeo real, utiliza toda la información obtenida y analizada de las dos fases anteriores para lanzar un ataque completo contra el sistema o la red en la que él intenta infiltrarse. Explota todas las vulnerabilidades expuestas y obtiene el control del sistema que ha sido pirateado. Ahora el "hacker" puede robar todos los datos que tiene disponibles, corromper los sistemas, agregar virus u otras entidades maliciosas, o manipularlos en su beneficio.

d) **La fase de mantenimiento del acceso**. Por lo general, los piratas informáticos tienen una misión que cumplir o un plan a seguir cuando piratean el sistema de una organización. Esto significa que simplemente ingresar o piratear el sistema no será suficiente. El "hacker" ético tiene que mantener su acceso al servidor hasta que cumpla su objetivo. Los "hackers" éticos suelen emplear troyanos y otras puertas traseras o "rootkits" para llevar a cabo esta fase. También pueden usar esta fase de acceso de mantenimiento para lanzar otros ataques para infligir más daño a la organización.

e) **La fase de cubrimiento de huellas**. Este es el paso final para completar todo el proceso de piratería ética. Si esta fase se completa con éxito, el "hacker" ético ha logrado piratear un sistema o red. Él podría infligir el mayor daño posible y ha

logrado dejar el sistema sin dejar rastro. Necesitan cubrir sus huellas en todo momento para evitar ser detectados al entrar y salir de la red o el servidor. Los sistemas de seguridad existentes no deberían poder identificar al atacante. La señal de un ciberataque simulado exitoso es si el sistema de seguridad nunca se dio cuenta de que se produjo un ataque por completo.

Esto incluye muchas de las siguientes medidas que un "hacker" ético toma para ocultar y eliminar su presencia por completo:

- Eliminación de todos los registros.
- Corrupción de registros.
- Modificar ciertos valores de "logs" o registros.
- Eliminar todas las carpetas que ha creado el "hacker" ético.
- Desinstalar todas las aplicaciones.
- Eliminar todo rastro de cualquier actividad realizada por un "hacker" ético en el sistema o red.

El "hacking" ético es un proceso largo y difícil que involucra muchas fases. Los profesionales que trabajan deben tener la capacitación y la certificación necesarias en piratería ética y seguridad de TI para convertirse en piratas informáticos éticos exitosos. Las fases requieren mucho tiempo, conocimiento y experiencia para llevarse a cabo y deben tomarse en serio. Las organizaciones también optan por personas certificadas sobre sus contrapartes no certificadas, porque están a cargo de proteger los datos confidenciales y los activos digitales de la empresa.

2.2. Técnicas

El desarrollo de la tecnología se puede ver en todas partes. Nadie puede negar que la tecnología está creciendo a un ritmo acelerado. Sin embargo, a medida que avanza la tecnología, existen problemas técnicos. La piratería ética se utiliza para prevenir amenazas de fuentes desconocidas. Hay varios tipos de técnicas de piratería ética. Uno puede aprender herramientas y técnicas éticas a través de varios cursos en línea y fuera de línea. Las herramientas se proporcionan para garantizar la seguridad de la información confidencial en la red y el sistema.

Hacking ético: un entendimiento

La piratería ética implica un sistema de piratería que depende de valores éticos o morales sin mala intención. Cualquier forma de piratería autorizada por el propietario del sistema de destino se conoce como piratería ética. Es el proceso de adaptar medidas de seguridad activas para defender los sistemas de piratas informáticos con malas intenciones con respecto a la privacidad de los datos.

Las técnicas de piratería ética proporcionan medidas de seguridad que un sistema aplica para buscar vulnerabilidades, infracciones y posibles amenazas a los datos. Un "hacker" ético piratea el sistema al que se ha dirigido antes que cualquier hacker. Por este motivo, se aplican parches de seguridad. Esto elimina y reduce efectivamente las posibilidades de que el atacante ejecute el "hack". Utilizando herramientas y técnicas de "hacking" ético, un "hacker" puede superar las amenazas buscando los puntos débiles del sistema. Estas herramientas se pueden utilizar para proteger los datos y sistemas del usuario. Brindan seguridad y protección. Existen diferentes tipos de métodos de "hacking" ético; algunos de ellos son los siguientes:

- “Hackers” de sombrero negro.
- “Hackers” de sombrero blanco.
- “Hackers” de sombrero gris.
- Varios piratas informáticos.

Video 3. Tipos de “Hackers”

Enlace de reproducción del video

Video 3. Síntesis del video: Tipos de “Hackers”
Los programadores informáticos reclaman que el término “hacker” se refiere a alguien con una comprensión avanzada de los computadores y las redes informáticas, mientras que “cracker” sería el término más apropiado para quienes irrumpen en las computadoras. Luego, entre esta clasificación se encuentran:

Sombreros negros: son aquellos que piratean para obtener acceso no autorizado a un sistema y dañar sus operaciones o robar información sensible.

Sombreros blancos: también son conocidos como "hackers" éticos. Nunca intentan dañar un sistema sino que tratan de encontrar las debilidades de una computadora o un sistema de red.

Sombreros grises: son una mezcla de "hackers" de sombrero negro y blanco. Actúan sin intención maliciosa pero para su diversión explotan una debilidad de seguridad en un sistema o red informática sin permiso o conocimiento del propietario.

Hacktivistas: utilizan la tecnología para anunciar un mensaje social, ideológico, religioso o político.

Los verificadores de sombrero blanco son piratas informáticos éticos, mientras que los piratas informáticos de sombrero negro se denominan piratas informáticos o "crackers" no autorizados. Utilizan diversas técnicas y métodos para proteger e interrumpir los sistemas de seguridad. Se puede recopilar la mayor cantidad de datos posible sobre sistemas y redes específicas a través de técnicas de huella y piratería ética. El paquete para un novato depende de la habilidad y el conocimiento.
Un "hacker" experimentado puede obtener buenos ingresos. Existe una gran demanda de "ethical hacking" en el mercado, y se está volviendo cada vez más popular. Si alguien quiere sobresalir en este campo, puede elegir la capacitación en "hacking" ético en línea.

Las mejores técnicas de piratería ética

La piratería ética tiene el potencial de probar, escanear y asegurar sistemas y datos. Las técnicas de piratería ética se pueden aprender utilizando un PDF de piratería ética y algunas de las técnicas se indican a continuación:

a) **Suplantación de identidad.** El "phishing" es un ataque de ciberseguridad en el que un hacker envía mensajes haciéndose pasar por una persona de confianza. Estos tipos de mensajes manipulan a un usuario, lo que hace que realice acciones como instalar un archivo malicioso y hacer clic en un enlace. Un "phisher" utiliza recursos públicos para recopilar información sobre la experiencia personal y laboral de la víctima. Luego usan esta información para crear un mensaje falso confiable.

b) **Rastrear.** La detección es el proceso de realizar un seguimiento y capturar todos los paquetes que pasan a través de una red determinada. Esto se hace usando algunas herramientas de rastreo. También se conoce como escuchas telefónicas, ya que puede escuchar y conocer la conversación. Un "sniffer" cambia la NIC del sistema al modo promiscuo.

c) **Ingeniería social.** La ingeniería social se utiliza para convencer a las personas de que revelen su información confidencial. El atacante engaña a las personas aprovechándose de su confianza y falta de conocimiento. Hay tres tipos de ingeniería social: basada en humanos, en dispositivos móviles y en computadoras. Debido a las políticas de seguridad laxas y la ausencia de herramientas de "hardware" o "software" para evitarlo, es difícil detectar un ataque de ingeniería social.

d) **Huella**. En esta técnica de piratería ética, el pirata informático recopila la mayor cantidad de datos posible sobre un sistema e infraestructura, para reconocer oportunidades para penetrarlos. El pirata informático puede usar varias herramientas y tecnologías para obtener información y descifrar un sistema completo.

e) **Inyección SQL**. La inyección SQL es un ataque en el que el atacante envía una consulta SQL, una declaración, a un servidor de base de datos que la modifica según sea necesario. Una inyección SQL ocurre cuando la entrada del usuario se sanea incorrectamente antes de usarla en una consulta SQL. SQL permite asegurar una respuesta de la base de datos. Ayudará al "hacker" a comprender la construcción de la base de datos, como los nombres de las tablas.

f) **Enumeración**. Enumeración también significa recopilación de información. En este proceso, el atacante crea una conexión con la víctima para encontrar tantos vectores de ataque que se utilicen para explotar el sistema en el futuro. Un "hacker" necesita establecer una conexión activa con el "host" de destino. En primer lugar, se cuentan y evalúan las vulnerabilidades. Luego, se hace para buscar ataques y amenazas para apuntar al sistema. Esto se utiliza para recopilar el nombre de usuario, los nombres de "host", las contraseñas y las direcciones IP.

Herramientas para ejecutar las técnicas perfectas de piratería ética

Hay muchas herramientas de piratería ética disponibles para la comodidad del usuario. Además, las herramientas de piratería ética ayudan en las investigaciones de seguridad.

a) **Ettercap.** Incluye las funciones de análisis de host y red. Además, Ettercap tiene la capacidad de rastrear una conexión SSH. Permite crear complementos personalizados utilizando API. Además, permitirá inyectar algunos caracteres en el servidor o en la red del cliente; también admite un análisis detallado de la acción junto con protocolos pasivos. Uno puede solicitar un programa de certificado de seguridad cibernética en línea para aprender una gestión y control de seguridad efectivos.

b) **Netsparker**. Es el escáner de seguridad de aplicaciones web más reciente que detecta automáticamente las vulnerabilidades en las aplicaciones web. Está disponible en forma de solución SAAS. Netsparker detecta vulnerabilidades muertas utilizando la última tecnología de escaneo. La herramienta requiere menos configuración; puede escanear más de 1.000 aplicaciones web en poco tiempo.

c) **Burp suite.** Es una de las herramientas de piratería ética que ayuda en las pruebas de seguridad. Esta característica es útil para probar aplicaciones web. Incluye una amplia gama de herramientas que ayudan en el proceso de prueba. La herramienta Burp Suite puede detectar el spam de alrededor de 2.000 aplicaciones web. También puede escanear aplicaciones de "software" de código abierto. Se utilizan para detectar errores y "malware" con precisión con la ayuda de herramientas de análisis avanzadas.

d) **John the Ripper.** Es una de las herramientas más populares para descifrar contraseñas. La herramienta se utiliza para probar la seguridad de la contraseña. Esta herramienta utiliza tecnología de fuerza bruta para hackear contraseñas, puede detectar automáticamente el tipo de cifrado

de la contraseña. Esta función la convierte en la mejor entre todas las demás herramientas para hackear claves. Esta herramienta utiliza algoritmos como MD4, LDAP, DES y Hash LM.

e) **Nmap.** Es una herramienta de seguridad de código abierto; esta se utiliza principalmente para gestionar y auditar la seguridad de redes y sistemas. Por lo general, los profesionales de seguridad de la información usan esta herramienta para encontrar "malware", auditorías de red, mapeo de red y más para hosts locales y remotos.

f) **Wireshark**. Se utiliza para analizar el tráfico de red en tiempo real. Esta herramienta es de código abierto para la piratería ética. Se incluyen diferentes funciones como GUI de potencia y navegador de paquetes, lo que da como resultado otros formatos. Además, la herramienta admite varios tipos de protocolos. Está disponible para diferentes sistemas operativos como Windows, Mac, etc.

g) **Open VAS**. Se utiliza para detectar vulnerabilidades en diferentes hosts. Es uno de los escáneres de red de código abierto. En esta herramienta se incluyen diferentes funciones, como una interfaz basada en web, escaneos programados y escaneo de múltiples hosts a la vez. Además, OpenVas está integrado con el software de monitoreo Nagios.

h) **Escáner Angry IP.** No requiere ninguna instalación. La herramienta escanea redes locales y web. Angry IP cuenta con las mejores técnicas de escaneo. La herramienta es de código abierto y gratuita, que admite diferentes plataformas. La herramienta ayuda a los piratas informáticos con soporte exclusivo.

i) **Iron**. La herramienta Iron es útil para las pruebas de "malware" de aplicaciones web. Es de código abierto y gratuito. Además, la herramienta es una herramienta basada en GUI fácil de usar. Los lenguajes de programación como Python y Ruby son compatibles con él. Esta herramienta proporciona informes en diferentes formatos como HTML y RTF. Esta herramienta puede comprobar cerca de 30 aplicaciones web.

j) **Acunetix**. Es una herramienta de piratería completamente automática. Esta herramienta se adelanta a cualquier intruso. Los problemas complejos relacionados con la web y la red se auditan en la herramienta. Varias características incluyen escanear diferentes variantes como inyección SQL, XSS, etc. Están disponibles tanto en las instalaciones como en plataformas en la nube.

Tipos de hacking ético

A continuación, se muestra la lista de diferentes tipos de "Hacking" Ético el cual hace referencia a la práctica que hace una persona altamente formada y con grandes conocimientos sobre informática y ciberseguridad, para ayudar a una empresa a detectar vulnerabilidades y debilidades:

- **Hackeo de aplicaciones web.** Los métodos utilizados son ataques de inyección SQL, secuencias de comandos entre sitios, comunicaciones inseguras, etc.
- **Ingeniería social.** Se utiliza para convencer a las personas de que revelen su información confidencial. El atacante engaña a las personas aprovechándose de su confianza y falta de conocimiento.

- **Hackeo del sistema**. La piratería del sistema es el sacrificio del “software” de la computadora para acceder y robar sus datos confidenciales. El “hacker” se aprovecha de las debilidades de un sistema informático para obtener la información y los datos y se aprovecha injustamente.
- **Hackeo de redes inalámbricas**. La piratería inalámbrica ataca redes inalámbricas o puntos de acceso que ofrecen información confidencial, como ataques de autenticación, acceso al portal de administración, contraseña wifi y otros datos similares. Se realiza para acceder a una red wifi privada.
- **Hackeo de servidores web**. Los piratas informáticos piratean servidores web para obtener ganancias financieras mediante el robo, el sabotaje, el chantaje, la extorsión, etc.

2.3. Consideraciones

La piratería ética se ha convertido en una forma esencial para que las empresas identifiquen y aborden las exposiciones a la seguridad cibernética. En este aparte de piratería ética, los especialistas en seguridad cibernética con sede en el Reino Unido, Redscan, describen la práctica como la identificación y explotación de vulnerabilidades de seguridad cibernética en entornos de TI con fines legítimos y no maliciosos.

La piratería ética es lo opuesto a la piratería de "sombrero negro", el tipo de piratería que aparece en los titulares de las noticias por las razones equivocadas. La piratería de sombrero negro es un delito y, si bien la piratería ética puede involucrar técnicas similares, generalmente la lleva a cabo una empresa profesional contratada para realizar pruebas y se adhiere a los más altos estándares. ¿Qué hace que la piratería

ética sea "ética"? Veamos cómo la piratería ética puede ayudar a proteger a las empresas de los ataques, además de examinar las formas en que puede asegurarse de que está trabajando con piratas informáticos éticos genuinos.

- **Realizado con consentimiento**. El "hacking" ético siempre se realiza con consentimiento. Si bien el objetivo de los compromisos es reproducir con precisión las tácticas, técnicas y procedimientos utilizados por los ciberdelincuentes, nunca está diseñado para ser malicioso y tiene como objetivo evitar daños e interrupciones en las empresas. Antes de realizar una evaluación, una firma profesional de ciberseguridad se asegurará de que exista un acuerdo formal que defina claramente el alcance de las evaluaciones y mantenga la confidencialidad del cliente.
- **Realizado por expertos**. La piratería ética siempre debe ser realizada por profesionales capacitados que comprendan las últimas herramientas y técnicas de piratería y realicen evaluaciones con los más altos estándares técnicos, legales y éticos. Es importante buscar organizaciones que tengan las certificaciones de piratería ética adecuadas: uno de los organismos de acreditación más conocidos y reconocidos es Crest. También es recomendable buscar firmas que tengan personal certificado con una amplia gama de disciplinas de piratería ética; esto demuestra la capacidad de la organización para realizar una amplia gama de evaluaciones.
- **Realizado por consultores con autorización de seguridad**. Al encargar una evaluación de piratería ética, es importante tener plena confianza en las personas involucradas. Cuando una prueba de penetración implica el acceso a información altamente confidencial o clasificada, las empresas

pueden considerar salvaguardas adicionales, como el uso de evaluadores con autorización de seguridad de alto nivel.

- **Realizado de acuerdo con las leyes vigentes.** Hay muchos aspectos legales que deben tenerse en cuenta al someterse a una piratería ética. Los evaluadores pueden, a través del proceso normal de un compromiso, acceder a datos altamente confidenciales. Para lograr un objetivo acordado, es posible que tengan la necesidad de filtrar esta información. Un negocio de piratería ética profesional considerará los problemas legales descritos en la legislación, incluidas las leyes en países/estados específicos y regulaciones como GDPR. Al programar cualquier forma de piratería ética, es aconsejable consultar al equipo legal de la organización para asegurarse de que las pruebas se mantengan dentro de lo permitido por la ley. Si bien ningún hacker ético tiene la intención de causar daños o interrupciones, existen riesgos inherentes a la realización de pruebas en sistemas en vivo: todas las partes deben ser conscientes de los riesgos y establecer las medidas de seguridad adecuadas.
- **Realizado de forma transparente.** Es esencial que las evaluaciones de piratería ética sean lo más transparente posible. Un "hacker" ético siempre compartirá los hallazgos y ofrecerá consejos de reparación para garantizar que las vulnerabilidades se informen y aborden. Deben ser localizables a lo largo de los compromisos y proporcionar informes escritos claros para resumir los hallazgos y las recomendaciones. Hay muchas cosas a considerar al encargar la piratería ética para el negocio. En cualquier caso, es una buena idea trabajar con un proveedor con mucha experiencia que esté feliz de explicarle cualquier riesgo y asegurarse de que todo el

proceso se lleve a cabo de la manera más segura posible y brinde resultados tangibles.

3. Mejoramiento continuo

Cuando se trata de administrar el desempeño de la seguridad cibernética de la organización, los líderes de seguridad y riesgo deben adoptar un enfoque basado en el riesgo y orientado a los resultados. Pueden hacerlo a través de mediciones dirigidas, monitoreo continuo y planificación y pronóstico detallados en un esfuerzo por reducir el riesgo cibernético de manera medible. El monitoreo continuo de la postura de seguridad de una organización es solo el comienzo en la construcción de un programa maduro de gestión del rendimiento de la seguridad. Las empresas deben ir más allá del monitoreo continuo para ser realmente efectivas: debe haber un proceso de mejora continua.

El concepto de mejora continua es la mejora continua de procesos a través de mejoras incrementales y revolucionarias. Estos esfuerzos pueden buscar un progreso "incremental" con el tiempo o una mejora "revolucionaria" todo a la vez. Si bien las mejoras innovadoras son efectivas, es la mejora incremental a lo largo del tiempo de los procesos y procedimientos de seguridad lo que conduce a un cambio efectivo a largo plazo. Son varios los principios que componen este modelo de mejora continua de la ciberseguridad, los cuales se detallan a continuación:

a) **Pequeños cambios pueden generar mejoras significativas**. Al administrar el rendimiento de seguridad, debe comenzar con una línea de base. Las métricas de rendimiento de referencia suelen ser la mejor manera de empezar a pensar en cómo adoptar un enfoque más basado en los resultados para gestionar el programa de seguridad de la organización. Para muchos líderes de seguridad y riesgo, las calificaciones de seguridad

se han convertido en esta medida de referencia de la eficacia del programa de seguridad general.

Pero entonces la pregunta es, ¿cómo mejora programáticamente esa medición de referencia con el tiempo? Al evaluar las áreas del programa en busca de fortalezas y debilidades, se puede identificar áreas de mejora; para lo cual, si la asignación de recursos debería conducir con el tiempo a mejoras incrementales en aquellas áreas débiles del programa.

b) **La retroalimentación de los empleados identifica oportunidades de mejora.** Muchas empresas inteligentes han implementado iniciativas de capacitación en concientización sobre seguridad para que los empleados asuman más responsabilidad por la ciberseguridad de su empresa. De hecho, la cultura de la empresa y el comportamiento de los empleados son dos de los factores clave que determinarán si una organización se vuelve más segura o menos vulnerable. Escuchar atentamente los comentarios de los empleados, ya que son los contribuyentes individuales que implementan muchas de estas medidas de seguridad, es fundamental para ver cómo mejora la postura de seguridad de una organización. En última instancia, el objetivo es crear una cultura de conciencia de seguridad; una empresa que tiene una cultura que se preocupa por la seguridad tendrá mejores procesos implementados, lo que conducirá a programas de seguridad mejores y más efectivos y a menos resultados negativos.

c) **Las mejoras incrementales generan valor a largo plazo**. Especialmente cuando se trata de ciberseguridad y calificaciones de seguridad, puede llevar tiempo que las acciones para remediar se hagan evidentes, tanto internamente como en su calificación de seguridad. La razón de esto es

que "arreglar problemas" es como un vendaje, simplemente encubre problemas en curso. Pero se necesita tiempo para comprender realmente cuál es el problema de la falla del proceso y cuál debería ser la solución correcta. Con el tiempo, la cantidad de problemas debería disminuir a medida que mejoran sus procesos, y seguirán tanto la mejora de su calificación como la eficacia del programa de seguridad.

3.1. Socialización de resultados del tratamiento de riesgo

El tratamiento del riesgo es el proceso de selección e implementación de medidas para modificar el peligro. Las medidas pueden incluir evitar, optimizar, transferir o retener el riesgo. Las medidas se utilizan dentro del Sistema de Gestión de Seguridad de la Información (SGSI) de la organización. En este nivel, las medidas de seguridad son descripciones verbales de diversas funciones de seguridad que se implementan técnicamente (por ejemplo, componentes de “software” o “hardware” u organizativas (por ejemplo, procedimientos establecidos).

Identificación de opciones

Una vez identificados y evaluados los riesgos, el siguiente paso consiste en la identificación de acciones alternativas adecuadas para la gestión de estos riesgos, la evaluación y valoración de sus resultados o impacto y la especificación e implementación de planes de tratamiento. Dado que los riesgos identificados pueden tener un impacto variable en la organización, no todos los riesgos conllevan la posibilidad de pérdida o daño. Las oportunidades también pueden surgir del proceso

de identificación de riesgos, a medida que se identifican los tipos con impacto o resultados positivos.

- Las opciones de manejo o tratamiento para los riesgos que se espera que tengan un resultado positivo incluyen:
- Iniciar o continuar una actividad que probablemente genere o mantenga estos resultados.
- Modificar la probabilidad del riesgo, para aumentar los posibles resultados beneficiosos.
- Tratar de manipular las posibles consecuencias, para aumentar las ganancias esperadas.
- Compartir el riesgo con otras partes que pueden contribuir proporcionando recursos adicionales que podrían aumentar la probabilidad de la oportunidad o las ganancias esperadas.
- Mantener el riesgo residual.

Las opciones de gestión para los riesgos con resultados negativos son similares a las de los riesgos con resultados positivos, aunque su interpretación e implicaciones son completamente diferentes. Tales opciones o alternativas podrían ser:

- Evitar el riesgo al decidir detener, posponer, cancelar, desviar o continuar con una actividad que puede ser la causa de ese riesgo.
- Modificar la probabilidad del riesgo tratando de reducir o eliminar la probabilidad de los resultados negativos.
- Tratar de modificar las consecuencias de manera que se reduzcan las pérdidas.

- Compartir el riesgo con otras partes que enfrentan el mismo riesgo, mediante acuerdos de seguros y estructuras organizativas como sociedades y empresas conjuntas, puede utilizarse para distribuir la responsabilidad. No obstante, es importante tener en cuenta que al compartir un riesgo, ya sea en su totalidad o en parte, la organización adquiere un nuevo riesgo, es decir, el riesgo de que la organización a la cual se ha transferido el riesgo inicial no lo gestione de manera eficaz.
- Retener el riesgo o sus riesgos residuales.

Es importante considerar todos los costos y beneficios directos e indirectos, ya sean tangibles o intangibles y medidos en términos financieros o de otro tipo. Se puede considerar y adoptar más de una opción por separado o en combinación. Un ejemplo es el uso eficaz de contratos de apoyo y tratamientos de riesgo específicos seguidos de seguros apropiados y otros medios de financiación del riesgo. En caso de que los recursos disponibles (por ejemplo, el presupuesto) para el tratamiento de riesgos no sean suficientes, el plan de acción de gestión de riesgos debe establecer las prioridades necesarias e identificar claramente el orden en que se deben implementar las acciones de tratamiento de riesgos individuales.

Desarrollo del plan de acción

Los planes de tratamiento son necesarios para describir cómo se implementarán las opciones elegidas. Los planes de tratamiento deben ser integrales y deben proporcionar toda la información necesaria sobre:

- Acciones propuestas, prioridades o planes de tiempo.
- Requerimientos de productos.

- Roles y responsabilidades de todas las partes involucradas en las acciones propuestas.
- Medidas de desempeño.
- Requisitos de información y seguimiento.

Los planes de acción deben estar en consonancia con los valores y las percepciones de todos los tipos de partes interesadas (por ejemplo, unidades organizativas internas, socios externos, clientes, etc.). Cuanto mejor se comuniquen los planes a las diversas partes interesadas, más fácil será obtener la aprobación de los planes propuestos y un compromiso con su implementación.

Aprobación del plan de acción

Al igual que con todos los procesos de gestión relevantes, la aprobación inicial no es suficiente para garantizar la implementación efectiva del proceso. El apoyo de la alta dirección es fundamental durante todo el ciclo de vida del proceso. Por ello, es responsabilidad del responsable del proceso de gestión de riesgos mantener continua y debidamente informada y actualizada a la dirección ejecutiva de la organización, a través de informes completos y periódicos.

Implementación del plan de acción

El plan de gestión de riesgos debe definir cómo se llevará a cabo la gestión de riesgos en toda la organización. Debe desarrollarse de manera que asegure que la gestión de riesgos esté integrada en todas las prácticas y procesos comerciales importantes de la organización para que sea relevante, eficaz y eficiente. Más específicamente, la gestión de riesgos debe integrarse en el proceso de desarrollo de políticas, en la planificación estratégica y empresarial, y en los procesos de gestión del

cambio. También es probable que esté integrado en otros planes y procesos, como los de gestión de activos, auditoría, continuidad del negocio, gestión ambiental, control de fraude, recursos humanos, inversión y gestión de proyectos.

El plan de gestión de riesgos puede incluir apartados específicos para determinadas funciones, áreas, proyectos, actividades o procesos. Estas secciones pueden ser planes separados, pero en todos los casos deben ser consistentes con la estrategia de gestión de riesgos de la organización (que incluye políticas de RM específicas por área de riesgo o categoría de riesgo). La conciencia necesaria y el compromiso con la gestión de riesgos en los niveles de alta dirección en toda la organización es fundamental para la misión y debe recibir una atención especial por parte de:

- Obtener el apoyo activo y continuo de los directores y altos ejecutivos de la organización para la gestión de riesgos y para el desarrollo e implementación de la política y el plan de gestión.
- Designar a un alto directivo para que dirija y patrocine las iniciativas.
- Conseguir la implicación de todos los altos directivos en la ejecución del plan.

El directorio de la organización debe definir, documentar y aprobar la política para la gestión de riesgos, incluidos los objetivos y una declaración de compromiso. La póliza puede incluir:

- Los objetivos y justificación de la gestión del riesgo.
- Los vínculos entre la política y los planes estratégicos de la organización.

- El alcance y los tipos de riesgo que asumirá la organización y las formas en que equilibrará las amenazas y las oportunidades.
- Los procesos que se utilizarán para gestionar el riesgo.
- Responsabilidades para gestionar riesgos particulares.
- Detalles del apoyo y la experiencia disponible para ayudar a los involucrados.
- Una declaración sobre cómo se medirá e informará el desempeño.
- Un compromiso con la revisión periódica del sistema.
- Una declaración de compromiso con la política por parte de los directores y ejecutivos de la organización.

La publicación y comunicación de una declaración de política de este tipo demuestra al entorno interno y externo de la organización, el compromiso de la junta ejecutiva con la gestión de riesgos y especifica claramente los roles y la responsabilidad a nivel personal. Los directores y altos ejecutivos deben ser los responsables últimos de la gestión del riesgo en la organización. Esto puede ser facilitado para:

- Especificar a los responsables de la gestión de riesgos particulares, de la implementación de estrategias de tratamiento y del mantenimiento de los controles.
- Establecer procesos de medición y presentación de informes de rendimiento.
- Asegurar niveles apropiados de reconocimiento, recompensa, aprobación y sanción.

Como se hace evidente, la implementación real de medidas de seguridad para la plataforma de TI subyacente no forma parte de esta actividad. Más bien, la implementación de planes de acción se refiere a las acciones a realizar para reducir los riesgos identificados. El trabajo necesario a nivel de implementación técnica de medidas de seguridad se realiza dentro del SGSI, es decir, fuera del proceso de gestión de riesgos.

Por último, pero no menos importante, una responsabilidad importante de la alta dirección es identificar los requisitos y asignar los recursos necesarios para la gestión de riesgos. Esto debe incluir personas y habilidades, procesos y procedimientos, sistemas de información y bases de datos, dinero y otros recursos para actividades específicas de tratamiento de riesgos.

Identificación de riesgos residuales

El riesgo residual es un riesgo que permanece después de que se hayan identificado las opciones de gestión de riesgos y se hayan implementado los planes de acción. También incluye todos los peligros inicialmente no identificados, así como todos los riesgos previamente identificados y evaluados, pero no designados para tratamiento en ese momento. Es importante que la dirección de la organización y todos los demás responsables de la toma de decisiones estén bien informados sobre la naturaleza y el alcance del riesgo residual. Para este propósito, los riesgos residuales siempre deben documentarse y someterse a procedimientos regulares de monitoreo y revisión.

3.2. Informe técnico de hallazgos y recomendaciones

Si se está pensando en obtener una evaluación de seguridad cibernética, es probable que tenga preguntas.

- ¿Se tienen vulnerabilidades que lo exponen a un ciberataque?
- ¿Se está utilizando la tecnología adecuada para la seguridad?
- ¿El equipo de TI tiene la experiencia en ciberseguridad que se necesita?
- ¿Está TI manejando todo lo que hay que hacer?

Una evaluación de seguridad cibernética puede responder esas preguntas, pero sin duda responderá preguntas que no se pensó en hacer, como: ¿está un empleado utilizando los recursos de la red para su trabajo secundario? O, ¿se está sufriendo un ataque cibernético en este momento?

Los ejecutivos que reciben esta información están muy contentos de recibirla, como se puede imaginar, pero los líderes empresariales también están encantados de saber:

- Si el "firewall" es el correcto y funciona correctamente.
- Si el personal es susceptible a la ingeniería social.
- Si pueden contar con los procesos de respaldo y recuperación de datos.
- Si la seguridad para su fuerza de trabajo remota es adecuada.
- Las evaluaciones de seguridad cibernética guían su plan de mejoras de seguridad.
- Lo que aprenda de su evaluación depende del tipo de evaluación realizada y sus objetivos particulares.

El propósito general de una evaluación de seguridad cibernética es brindar una visión objetiva del estado de seguridad en este momento. Esto le brinda la información que necesita para hacer un plan de mejora, hacer que las actividades de seguridad sean más eficientes, presupuestar efectivamente la seguridad o incluso calificar para un seguro cibernético. La pregunta es: ¿cómo sería el plan de mejora? Aquí hay algunas recomendaciones comunes que provienen de las evaluaciones cibernéticas.

Recomendaciones comunes de evaluación de la seguridad cibernética:

a) **Implementar mejores prácticas para actualizaciones de "**software**"**. El "software" sin parches y sin soporte crea vulnerabilidades de seguridad. Los ciberdelincuentes utilizan programas que buscan equipos conectados a internet que tengan "software" antiguo y sin parches. Si tienen éxito en la explotación de estas vulnerabilidades, les da una puerta trasera a la computadora afectada y las redes corporativas. Mantener el "software" actualizado y nunca usar "software" sin soporte es una buena práctica que mantiene esas puertas traseras cerradas.
b) **Actualizar y administrar adecuadamente los "firewalls".** Los cortafuegos continúan siendo una capa de protección imprescindible en la estrategia de seguridad cibernética. Los cortafuegos faltantes o de baja calidad no harán el trabajo para mantener el tráfico no deseado fuera de la red y pueden convertirse en un punto de falla para toda la red si se cae. Además, si tiene un "firewall" moderno, la forma en que está configurado y administrado marca una gran diferencia en la eficacia.
c) **Control del tráfico de la red.** Se supone que la seguridad controla el tráfico de la red, pero la evaluación cibernética puede encontrar puertos abiertos,

conmutadores no administrados, controladores de dominio faltantes o incluso servidores de acceso público que pueden dejar la red vulnerable y abierta a un ataque.

d) **Implementar la detección y respuesta de punto final (EDR).** Antes, lo mejor que podía hacer con respecto a la detección de amenazas era reconocer las amenazas conocidas. Infortunadamente, eso ya no es lo suficientemente bueno. Debido a que los ciberdelincuentes utilizan la inteligencia artificial (IA) para crear continuamente nuevas tácticas, las defensas deben ser igual de inteligentes. End Point Detection and Response (EDR) es una capa imprescindible de la estrategia moderna de seguridad cibernética. Las herramientas EDR aprenden los patrones regulares de la red para que cuando ocurra algo fuera de lo común, como una intrusión cibernética, pueda solucionarlo de inmediato.

e) **Actualizar el filtro de spam de correo electrónico**. El filtro de spam básico del proveedor de correo electrónico no es suficiente para evitar los correos electrónicos de "phishing" que atraen a la gente para que descargue "malware". Incluso si se tiene un excelente proveedor de correo electrónico como Microsoft 365, configurar el filtro de correo no deseado requiere algo de experiencia, para permitir que ingrese el correo electrónico que desea.

f) **Implementar la autenticación de múltiples factores**. La gestión de contraseñas es una forma sencilla de mantener la seguridad de las cuentas, pero muchas personas consideran que es un inconveniente cambiar regularmente las contraseñas o utilizar contraseñas que no se descifren fácilmente.

g) **Mejorar los procesos de copia de seguridad y recuperación de datos.** Demasiadas empresas han tratado de usar los datos respaldados para recuperarse de un incidente cibernético solo para descubrir que la cantidad de datos que podían recuperar era inadecuada o, peor aún, no estaba allí en absoluto. Los procesos de respaldo y recuperación de datos deben formularse para las necesidades comerciales.

h) **Actualizar y documentar políticas de seguridad**. La estrategia de seguridad cibernética incluye capas técnicas y no técnicas. Las capas no técnicas tienen que ver con la forma en que las personas acceden a los datos y las redes. Si bien a veces puede usar medios técnicos para restringir el acceso, es vital que se documente las expectativas y los permisos para ese acceso, y cumplir las prácticas aceptables que coincidan con los procesos comerciales.

i) **Comenzar la capacitación de concientización sobre seguridad cibernética**. En un mundo donde el 90% de todos los ataques cibernéticos implican ingeniería social, es vital que todos en la empresa, incluidos los ejecutivos, sepan cómo reconocer y responder a posibles ataques cibernéticos. Una vez al año el entrenamiento no es suficiente. La única forma de mantener la seguridad en la mente de los empleados es hacer que participen en una capacitación continua.

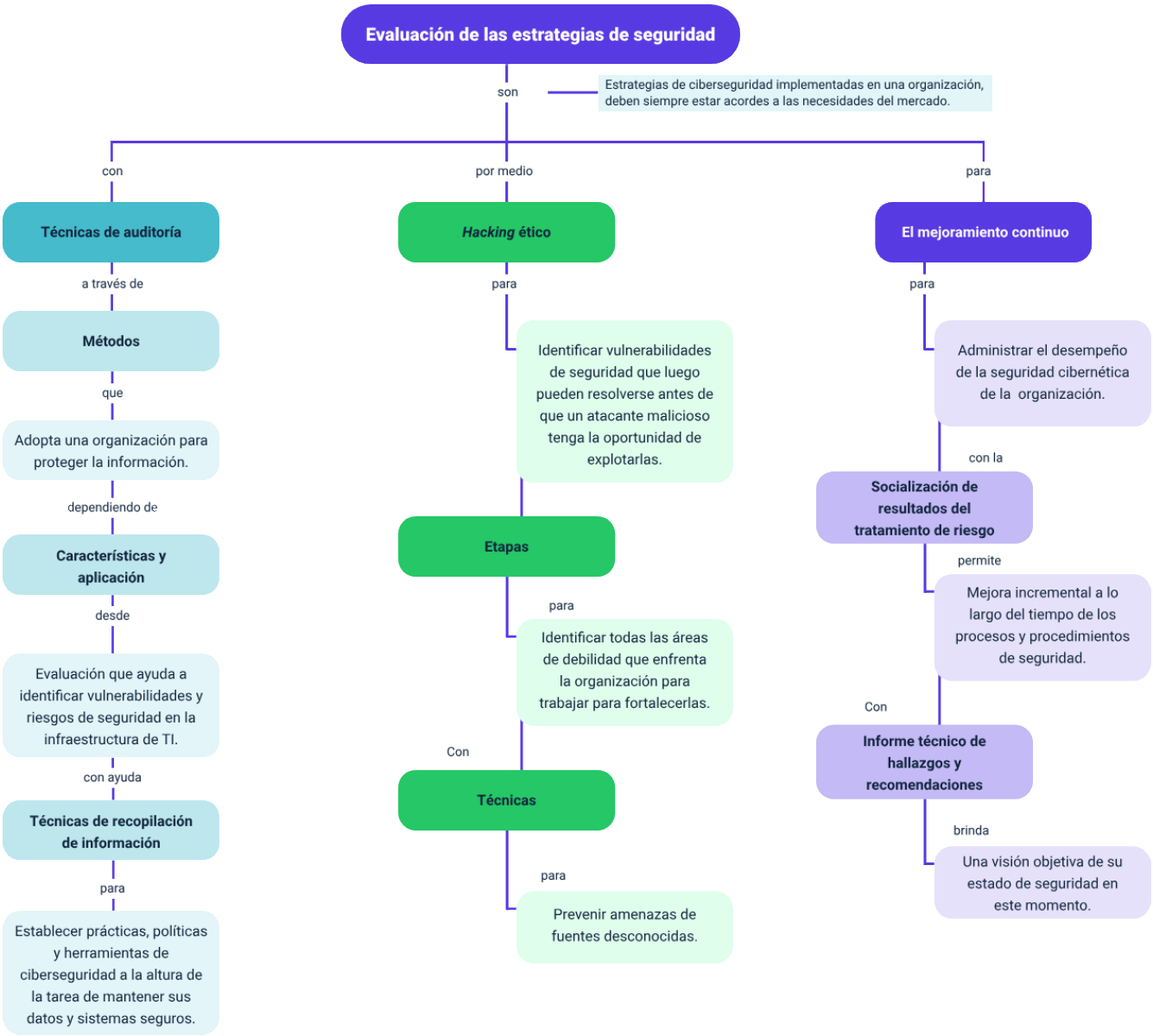
j) **Mejorar la seguridad física**. El entorno físico donde trabaja la gente también debe tenerse en cuenta en las estrategias de seguridad. Es posible que se deba mejorar la forma en que supervisa y permite el acceso a las instalaciones, y estar más al tanto de las idas y venidas de visitantes y proveedores que no necesitan estar atentos a los datos o configuración de

red. Además, ya sea que estén en la oficina o trabajando desde casa, los empleados deben bloquear las computadoras cuando se ausentan.

Nota. ¿Es hora de tener servicios de seguridad cibernética subcontratados? Con las recomendaciones que se obtienen de una evaluación de seguridad cibernética, surge otra pregunta: ¿es hora de externalizar los servicios de seguridad? La seguridad cibernética se ha convertido en una disciplina propia y requiere un enfoque del 100% para mantenerse al día con todas las tendencias y tácticas en evolución. Incluso si al equipo de TI le está yendo bien con la administración de la red, es posible que no tenga el conocimiento profundo para liderar la seguridad.

Síntesis

A continuación, se presenta un mapa conceptual que sintetiza el componente formativo:



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
Pruebas de Penetración	Mike James (2022). Ethical hacking (also referred to as white hat hacking) has become an essential way for businesses to identify and address cybersecurity exposures. Stay Safe Online.	Página web	https://staysafeonline.org/cybersecurity-for-business/how-can-ethical-hacking-be-ethical/#:~:text=Ethical%20hacking%20is%20always%20performed,damage%20and%20disruption%20to%20businesses
Técnicas de auditoría	Currentware. (2022). 7 Tips for Passing Your Next Cybersecurity Audit (Meet Compliance). Currentware.	Página web	https://www.currentware.com/blog/it-security-audit-tips/
Características de una buena auditoría	Immunebytes. (2022). Características de un buen auditor de seguridad cibernética. Immunebytes.	Página web	https://www.immunebytes.com/blog/traits-cyber-security-auditor/

Glosario

“Adware”: “software” que se apoya en anuncios (normalmente para financiarse) como parte del propio programa. En algunos casos se les considera “malware”. Es común en las versiones gratuitas en las aplicaciones.

Agujero de seguridad: fallo en un sistema de información que se puede explotar para violar la seguridad del sistema.

Amenaza: circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.

Análisis de riesgos: proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas para determinar los controles adecuados para tratar el riesgo.

“Antispyware”: herramienta de “software” diseñada para detectar y eliminar programas maliciosos del tipo “spyware” cuyo objetivo es espiar y obtener de forma sigilosa información personal presente en el dispositivo sin consentimiento del usuario.

Auditoría de seguridad: consiste en el análisis y gestión de sistemas llevado a cabo por profesionales en tecnologías de la información (TI) principalmente para identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones.

"Backup": copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados.

Biometría: método de reconocimiento de personas basado en sus características fisiológicas (huellas dactilares, retinas, iris, cara, etc.) o de comportamiento (firma, forma de andar, tecleo, etc.).

***Botnet*:** conjunto de ordenadores (denominados "bots") controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam, ataques de DDOS, etc.

Captcha: acrónimo en inglés de "Completely Automated Public Turing Test To Tell Computers and Humans Apart"; en español, prueba de "Turing" completamente automática y pública para diferenciar ordenadores de humanos, es un tipo de medida de seguridad que consiste en la realización de pruebas desafío-respuesta controladas por máquinas que sirven para determinar cuándo el usuario es un humano o un "bot" según la respuesta a dicho desafío.

Cortafuegos: la funcionalidad básica de un cortafuego es asegurar que todas las comunicaciones entre la red e internet se realicen conforme a las políticas de seguridad de la organización o corporación.

Disponibilidad: capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando estos lo requieran.

Gestión de incidentes: listado de procedimientos previamente documentados sobre los pasos a seguir en caso de detectar una amenaza de ciberseguridad en la empresa.

Referencias bibliográficas

Bitsight. (2019). The Importance of Continuous Improvement in Security Performance Management. https://www.bitsight.com/blog/importance-continuous-improvement-security-performance-management

Eccouncil (s.f). What is Ethical Hacking? https://www.eccouncil.org/ethical-hacking/

GlobalSign Blog. (2022). Comment (et pourquoi) mener des audits de cybersécurité dans votre entreprise. https://www.globalsign.com/fr/blog/comment-et-pourquoi-mener-des-audits-de-cybersecurite

Howard Poston. (2019) Information Collection in Cybersecurity. https://resources.infosecinstitute.com/topic/information-collection-in-cybersecurity/

Incibe. (s. f.). Glosario de términos de ciberseguridad. Gobierno de España. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Ingrid Horvath (2022). The Five Phases of Ethical Hacking. https://www.invensislearning.com/blog/phases-of-ethical-hacking/

Mon-infra. (s. f.). Quelles sont les étapes d'un audit informatique?

Premier IT Solution. (2022). External IT Security Audit - What It Is and Why You Need On. https://securityboulevard.com/2022/08/what-is-a-cybersecurity-audit-and-why-is-it-important/

Synopsys. (2022). Ethical Hacking. https://www.synopsys.com/glossary/what-is-ethical-hacking.html

Zevenet. (2021). 10 Importance of Information Security Audit.
https://www.zevenet.com/blog/10-importance-of-information-security-audit/

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal	Responsable del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Hernando José Peña Hidalgo	Experto Temático	Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander
Diego E. Acevedo Guevara	Diseñador Instruccional	Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander
Andrés Felipe Velandia Espitia	Asesor Metodológico	Centro de Diseño y Metrología - Regional Distrito Capital
Darío González	Corrector de Estilo	Centro de Diseño y Metrología - Regional Distrito Capital
Juan Daniel Polánco Muñoz	Diseñador de Contenidos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Francisco José Lizcano Reyes	Desarrollador Full-Stack	Centro Industrial del Diseño y la Manufactura - Regional Santander
Camilo Andrés Bolaño Rey	Locución	Centro Industrial del Diseño y la Manufactura - Regional Santander
Wilson Andrés Arenales Cáceres	Storyboard e Ilustración	Centro Industrial del Diseño y la Manufactura - Regional Santander
Mary Jeans Palacio Camacho	Animador y Productor Audiovisual	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruíz Torres	Validación de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Regional y Centro de Formación
Luis Gabriel Urueta Alvarez	Validación de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniel Ricardo Mutis	Evaluador para Contenidos Inclusivos y Accesibles	Centro Industrial del Diseño y la Manufactura - Regional Santander