Centro de la versión 1.0 para Seguridad en Internet ® Riesgo Método de evaluación

Para una implementación razonable y Evaluación de CIS Controls ™

Página 2

RAM CIS - Método de evaluación de riesgos del Centro de seguridad de Internet ® (Versión 1.0)

Abril 2018

Antecedentes y Agradecimientos

El contenido original de CIS RAM fue desarrollado por HALOCK Security Labs. Se basa en su Amplia experiencia ayudando a clientes y autoridades legales a lidiar con la seguridad cibernética cuestiones. Reconociendo la necesidad universal de un enfoque neutral de proveedor, abierto y de toda la industria para estos problemas, HALOCK Security Labs se acercó a CIS para hacer que este trabajo esté abiertamente disponible para el toda la comunidad de ciberseguridad. Esta generosa contribución de la propiedad intelectual (y el Se ha donado a CIS un extenso trabajo para generalizarlo y adaptarlo a los Controles CIS). ahora disponible y mantenido como una mejor práctica apoyada por la comunidad CIS.

Al igual que con todo el trabajo de CIS, agradecemos sus comentarios y también los voluntarios que deseen participar en la evolución de este y otros productos CIS.

CIS agradece las contribuciones proporcionadas por HALOCK Security Labs y el DoCRA Council en el desarrollo de CIS RAM y el CIS RAM Workbook.

Contribuciones significativas a la Versión 1 de CIS RAM fueron hechas por:

Autor principal:
Chris Cronin. Socio, laboratorios de seguridad HALOCK

Autores contribuyentes:
Jim Mirochnik, Terry Kurzynski y David Andrew, socios, laboratorios de seguridad HALOCK. Erik Leach y Steve Lawn, HALOCK Security Labs. Paul Otto, abogado, Hogan Lovells US LLP.

La revisión y la verificación fueron proporcionadas por múltiples miembros del personal del CIS.

Página 3

Tabla de contenido

Página 4

Página 5

Prefacio

El objetivo del Método de evaluación de riesgos del Centro para la seguridad en Internet ® ("CIS RAM") es ayudar las organizaciones planean y justifican su implementación de CIS Controls ™ Versión 7, ya sea que los controles están operando total o parcialmente. Pocas organizaciones pueden aplicar todos los controles a toda la información. activos, porque - mientras se reducen algunos riesgos - los controles de seguridad también introducen nuevos riesgos para eficiencia, colaboración, utilidad, productividad o fondos y recursos disponibles.

Las leyes, regulaciones y estándares de seguridad de la información consideran la necesidad de equilibrar la seguridad. contra el propósito de una organización y sus objetivos, y requieren evaluaciones de riesgos para encontrar y documentar ese saldo. El método de evaluación de riesgos descrito aquí proporciona una base para comunicación de riesgos de ciberseguridad entre profesionales de seguridad, gestión empresarial, legal autoridades y reguladores que usan un lenguaje común que es significativo para todas las partes.

La RAM CIS se ajusta y complementa la evaluación de riesgos de seguridad de la información establecida estándares, como ISO / IEC 27005, [1] NIST Publicación especial 800-30, [2] y RISK IT. [3] por

conforme a estos estándares, la RAM CIS ayuda al lector a realizar evaluaciones de riesgos
De acuerdo con las normas establecidas. Al complementar estos estándares, la RAM CIS ayuda a su
los lectores evalúan los riesgos y las salvaguardas utilizando el concepto de "cuidado debido" y "razonable
salvaguardas "que la comunidad legal y los reguladores usan para determinar si las organizaciones actúan
como una "persona razonable".

El CIS ® diseñó y priorizó los controles del CIS para que pudieran prevenir o detectar al máximo
Causas comunes de eventos de ciberseguridad según lo determinado por una comunidad de seguridad de la información
profesionales Como resultado, CIS Controls V7 tiene consideraciones de riesgo en su núcleo.

Pero debido a que los riesgos varían de una organización a otra, los métodos de análisis de riesgos descritos en
Este documento puede ayudar a las organizaciones a aplicar los Controles CIS para que puedan
aborde de manera defendible los riesgos y recursos únicos en cada organización.

Para quién es este método de evaluación de riesgos

Las evaluaciones de riesgos de ciberseguridad son herramientas importantes para las organizaciones que les ayudan a evaluar y priorizar sus riesgos, pero también determinar cuándo sus riesgos son aceptables. Esta evaluación de riesgos.
El método está diseñado para ser práctico para una amplia población de usuarios, ya sean principiantes
problemas de ciberseguridad, capaces de reconocer preocupaciones de ciberseguridad, o expertos.

Organizaciones que deben demostrar salvaguardas "razonables" y gestión de riesgos para
fines de gestión reglamentarios, contractuales o de seguridad pueden beneficiarse del uso de
método. Además, la RAM CIS está diseñada para promover comunicaciones significativas y
consenso entre técnicos, gestión no técnica, expertos en seguridad, gestores de riesgos, como
así como profesionales legales y reguladores.

[1] ISO / IEC 27005: 2011 proporcionado por la Organización Internacional de Normalización.

[2] Publicaciones especiales NIST 800-30 Rev. 1 proporcionadas por el Instituto Nacional de Normas y Tecnología.

[3] RIESGO IT Framework proporcionado por ISACA.

Página 6

Lo que proporciona este documento

El CIS RAM guía a los lectores a realizar evaluaciones de riesgos de una manera que coincida con las expectativas declarado en las leyes, reglamentos y normas de seguridad de la información. El CIS RAM logra esto
al proporcionar instrucciones, plantillas, ejemplos y ejercicios para demostrar sus métodos. Estas
fundamentar el marco de una evaluación de riesgos.

El papel del juicio profesional.

Usando CIS RAM, el lector podrá desarrollar rápidamente un registro de riesgos que comunique
razonabilidad para muchas autoridades y expertos, pero el lector también tendrá que traer su
juicio profesional (suyo y del juicio de expertos colaboradores) a la tarea.

El juicio profesional ayudará a las organizaciones a determinar el alcance y los límites del riesgo.
evaluación, para definir la misión, los objetivos y las obligaciones de la organización, para decidir qué
se evaluarán los riesgos, para identificar amenazas previsibles y recomendar un tratamiento de riesgos
salvaguardas

Página 7

Introducción del autor

La comunidad de seguridad de la información, los reguladores, los abogados y los gerentes entienden que La ciberseguridad perfecta no es posible. Incluso cuando las organizaciones implementan salvaguardas que son tan Práctico como CIS Controls V7, existen limitaciones en el grado en que las organizaciones pueden implementar salvaguardas de seguridad. Recursos de seguridad limitados (dinero, expertos y tiempo), negocios competidores prioridades y el panorama de amenazas en constante cambio dificultan que las organizaciones puedan implementar un estándar de ciberseguridad por igual para todos los activos de información.

Incluso sin estos desafíos, las organizaciones deben operar en entornos algo vulnerables. para cumplir su misión y alcanzar sus objetivos. Por ejemplo, el valor de seguridad del cifrado es obvio, sin embargo, la información en algún momento debe estar sin cifrar para cumplir su propósito. Y aveces la información debe estar sin cifrar para hacer cumplir otras salvaguardas de seguridad, como la pérdida de datos prevención. Pero, ¿cómo sabe una organización si acepta el riesgo de esos momentos y transacciones cuando la información no está encriptada? ¿Y cómo determina si otro ¿Las salvaguardas de apoyo protegen adecuadamente la información no cifrada? No hay respuesta única a esa pregunta u otras preguntas de ciberseguridad de “área gris” que las organizaciones encuentro regular. Para ayudar a las organizaciones en sus esfuerzos de seguridad, leyes, reglamentos, los tribunales, y los profesionales de seguridad de la información nos dicen que usemos evaluaciones de riesgos *para responder por nosotros mismos* si debemos aceptar o reducir los riesgos.

Las salvaguardas de ciberseguridad deben ser razonables y apropiadas. Deben reducir el riesgo de daño a las organizaciones y a otros, pero tampoco deben crear una carga demasiado grande sobre el organizaciones que usan esas salvaguardas. Se cargan los términos "razonable" y "apropiado" con muchos significados legales, regulatorios, de expertos y comerciales. Pero estos significados pueden ser abordado, documentado y justificado mediante una evaluación de riesgos bien construida.

Al utilizar la RAM CIS como parte de su programa de ciberseguridad, las organizaciones podrán más adopte los controles CIS V7 de una manera que pueda demostrarse con éxito como razonable y apropiado para la administración interna, autoridades, expertos en seguridad y asesores legales que tienen un interés en el éxito de la organización.

El documento RAM CIS está diseñado para guiar a las organizaciones paso a paso a través de su riesgo.

evaluación, independientemente de su experiencia en la realización de estas evaluaciones. Alentamos lectores para trabajar en cada capítulo que sea adecuado para su organización, y seguir junto con los ejercicios, hojas de trabajo y ejemplos hasta que se complete su registro de riesgos.

Chris Cronin

Socio, laboratorios de seguridad HALOCK

Presidente del Consejo DoCRA

Página 8

Estructura del documento

El Método de evaluación de riesgos de seguridad del Centro para Internet ® (CIS RAM) es un proceso documentado para realizar evaluaciones de riesgos que aborden los requisitos de seguridad, negocios, regulaciones y requisitos de deber de cuidado. Este documento describirá el método de evaluación de riesgos utilizando el siguientes componentes:

- Las instrucciones son la mayor parte de la RAM CIS. Las instrucciones proporcionan una guía paso a paso. para realizar una evaluación de riesgos como proyecto. Se proporcionan tres conjuntos de instrucciones que abordar el método de evaluación de riesgos para organizaciones basado en su gestión de riesgos madurez. Las instrucciones pueden ser personalizadas y adaptadas por cada organización según a sus necesidades. Las técnicas de evaluación de riesgos se proporcionan al final del documento para ayudar Las organizaciones desarrollan aún más sus capacidades de evaluación de riesgos.
- Los principios establecen las reglas necesarias y fundamentales para evaluar los riesgos de acuerdo con esto método. Los principios son las características fundamentales de una evaluación de riesgos que traduce las preocupaciones de seguridad a las expectativas regulatorias, legales y comerciales. Como organizaciones personalizar instrucciones y plantillas para su organización, estos principios deben permanecer. Procesos de evaluación de riesgos que se desarrollan y realizan sin apegarse a estos. los principios no pueden considerarse como "conformes" al método.
- Los ejemplos demuestran procesos y pasos. Los ejemplos irán acompañados de explicativos escenarios para mostrarle al lector cómo se debe llevar a cabo cada paso. Se proporcionan ejemplos tanto en este documento, y en un documento separado, el *CIS_RAM_Workbook* para facilitar su uso.
- Las plantillas modelan los pasos de evaluación de riesgos, los métodos de análisis de riesgos y los informes. Plantillas ayudará a la adopción rápida de los procesos del método por cada organización y proporcionará para prácticas consistentes de evaluación de riesgos entre organizaciones. Las plantillas se proporcionan en un documento separado, el *CIS_RAM_Workbook* para una fácil adopción de CIS RAM.
- Los ejercicios alientan al lector a aplicar lo que aprendió en las instrucciones utilizando el proporcionó plantillas para diseñar y realizar su propia evaluación de riesgos.
- Las notas de antecedentes explican por qué se toma un paso de evaluación de riesgos o por qué se aplica un principio. Los comentarios de fondo permiten a los profesionales de riesgos describir a las partes interesadas cómo La evaluación de riesgos aborda las necesidades de las partes interesadas y las autoridades.
- El Glosario proporciona definiciones de términos especializados utilizados en este documento. Porque el riesgo Los métodos de gestión varían y el público tiene una experiencia variable en la gestión de riesgos. El glosario garantizará el uso y el significado de términos consistentes.

-

Esta guía incluye referencias a una selección de controles de CIS Controls V7 como ejemplos de salvaguardas que se seleccionan específicamente para ayudar a proteger las organizaciones. Dado que tales recursos cambiar de vez en cuando, comuníquese con CIS o consulte nuestro sitio web para obtener la información más reciente información. (www.cisecurity.org)

Página 9

Glosario

Apropiado: una condición en la cual los riesgos para los activos de información no previsiblemente generarán daños que es mayor de lo que la organización o las partes interesadas pueden tolerar.

Clase de activo: Un grupo de activos de información que se evalúan como un conjunto en función de su similitud. "Servidores", "computadoras de usuario final", "dispositivos de red" son ejemplos, como son "servidores de correo electrónico", "web servidores "y" servidores de autenticación ".

Ruta de ataque: una serie de actividades y activos de información dentro del ciclo de vida de un incidente de seguridad.

Modelo de ruta de ataque: una descripción de cómo puede ocurrir una ruta de ataque específica dentro de un entorno.

Carga: El impacto negativo que una salvaguarda puede representar para la organización o para otros.

Propietarios de negocios: personal que posee procesos comerciales, bienes o servicios que contienen información soporte de tecnologías. es decir, gerentes de servicio al cliente, gerentes de producto, gestión de ventas.

Componentes: Individuos u organizaciones que pueden beneficiarse de una seguridad efectiva sobre activos de información, o pueden verse perjudicados si falla la seguridad.

Control: un método documentado para proteger los activos de información utilizando técnicas, físicas o garantías procesales.

Objetivo de control: el resultado previsto de un control.

Cuidado debido: la cantidad de cuidado que una persona razonable tomaría para evitar daños previsibles a otros.

Deber de cuidado: la responsabilidad de garantizar que no se produzcan daños a otros mientras se realiza actividades, ofrecer bienes o servicios, o realizar cualquier acto que previsiblemente pueda dañar a otros.

Impacto: el daño que puede sufrir cuando una amenaza compromete un activo de información.

Puntuación de impacto: la magnitud del impacto que puede sufrir. Esto se afirma en lenguaje sencillo y está asociado con escalas numéricas, generalmente de '1' a '3' o '1' a '5'.

Tipo de impacto: una categoría de impacto que estima la cantidad de daño que puede afectar a una parte o a proposito. La RAM CIS describe tres tipos de impacto; Misión, objetivos y obligaciones.

Activo de información: información o los sistemas, procesos, personas e instalaciones que facilitan manejo de información.

Riesgo inherente: la probabilidad de que ocurra un impacto cuando una amenaza compromete a un desprotegido activo.

Indicador clave de riesgo: agregaciones y análisis de tendencias de medidas que la administración puede usar para entender su estado de riesgo.

Probabilidad: el grado en que se espera que una amenaza genere un impacto. Puede expresarse en términos de frecuencia, previsibilidad o probabilidad.

Medida: Una indicación repetible y basada en evidencia de que una salvaguarda logra su objetivo de control.

Riesgo observado: El riesgo actual tal como le parece al evaluador de riesgos.

Probabilidad: el producto del análisis estadístico que estima la probabilidad de un evento.

Razonable: una condición en la cual las salvaguardas no crearán una carga para la organización que es mayor que el riesgo contra el cual está destinado a proteger.

Riesgo residual: el riesgo que queda después de aplicar una salvaguarda. Este concepto no se usa directamente por CIS RAM, pero implica que el riesgo se reduce cuando se aplica una salvaguarda. El riesgo residual no tener en cuenta los posibles impactos negativos para la organización cuando se aplican las salvaguardas.

Riesgo: una estimación de la probabilidad de que una amenaza cree un impacto no deseado. En términos de En este método, el riesgo puede expresarse como el producto de una probabilidad y un impacto.

Página 10

Análisis de riesgos: el proceso de estimar la probabilidad de que un evento cree un impacto. los la previsibilidad de una amenaza, la efectividad esperada de las salvaguardas y un resultado evaluado son componentes necesarios del análisis de riesgos. El análisis de riesgos puede ocurrir durante un riesgo integral evaluación, o como parte de otras actividades como gestión de cambios, vulnerabilidad evaluaciones, desarrollo y adquisición de sistemas, y excepciones de políticas.

Evaluación de riesgos: un proyecto integral que evalúa la posibilidad de que ocurra daño dentro de un alcance de los activos de información, controles y amenazas.

Evaluación de riesgos: el componente matemático del análisis de riesgos que estima la probabilidad y impacto de un riesgo, y lo compara con un riesgo aceptable.

Gestión de riesgos: un proceso para analizar, mitigar, supervisar y reducir riesgos.

Opción de tratamiento de riesgos: la selección de un método para abordar los riesgos. Las organizaciones pueden elija Aceptar, Reducir, Transferir o Evitar riesgos.

Plan de tratamiento de riesgos: un plan de proyecto integral para implementar el tratamiento de riesgos recomendaciones

Recomendaciones de tratamiento de riesgos: una lista de salvaguardas o procesos que pueden ser implementado y operado para reducir la probabilidad y / o impacto de un riesgo.

Protección: tecnologías, procesos y protecciones físicas que previenen o detectan amenazas. contra activos de información. Las salvaguardas son implementaciones de controles.

Riesgo de salvaguarda: El riesgo que representan las salvaguardas recomendadas. La misión de una organización o Los objetivos pueden verse afectados negativamente por un nuevo control de seguridad. Estos impactos deben ser evaluado para comprender su carga sobre la organización y para determinar si la carga es razonable.

Seguridad: una garantía de que las características de los activos de información están protegidas. Confidencialidad La integridad y la disponibilidad son características de seguridad comunes. Otras características de la información. activos como la velocidad, la autenticidad y la confiabilidad también pueden considerarse si son valiosos a la organización y sus constituyentes.

Estándar de atención: un conjunto de prácticas, controles o requisitos que se sabe que mejoran resultados y reducir fallas para los profesionales de un campo especializado o profesión.

Mayordomo: personal responsable de la seguridad y el correcto funcionamiento de la información. activos (por ejemplo, administrador de base de datos, administrador de registros o ingeniero de red).

Amenaza: un evento potencial o previsible que podría comprometer la seguridad de los activos de información.

Modelo de amenaza: una descripción de cómo una amenaza podría comprometer un activo de información, dada la salvaguardas y vulnerabilidades actuales en torno al activo.

Vulnerabilidad: una debilidad que podría permitir que una amenaza comprometa la seguridad de la información. bienes.

Página 11

Ejemplos de métodos de evaluación de riesgos

CIS RAM proporciona tres conjuntos de instrucciones que describen un proyecto completo de evaluación de riesgos. Cada conjunto de instrucciones está diseñado para organizaciones de gestión de seguridad de la información variable. capacidades para aumentar la utilidad del método.

Los tres conjuntos de instrucciones presentan una organización ficticia que está llevando a cabo una información. evaluación de riesgos de seguridad, y eso mejora sus capacidades de gestión de riesgos con el tiempo. los ejemplo organización comienza la evaluación de riesgos en el primer conjunto de instrucciones como seguridad principiante con poca participación de la gestión empresarial. Después de un año de mejorar su seguridad. postura y habilidades, evalúan el riesgo en el segundo conjunto de instrucciones utilizando más refinado razonamiento y métodos, y en colaboración con la gestión empresarial. Finalmente maduran suficiente como organización capaz de asumir análisis de riesgos complejos en el tercer conjunto de instrucciones.

La organización de ejemplo descrita en este documento fabrica y presta servicios médicos. dispositivos ("dispositivos de agenda") que leen información biológica de pacientes que usan los dispositivos. los La organización trabaja en entornos clínicos para apoyar a los pacientes, así como a los dispositivos, y un resultado lleva información de salud privada sobre los pacientes. Porque trabajan con militares y organizaciones de veteranos, muchos de sus pacientes son miembros activos o anteriores de las fuerzas armadas. Como resultado, la organización plantea un mayor riesgo y requiere un mayor escrutinio sobre sus controles de ciberseguridad.

La organización de ejemplo es hipotética y no se basa en una organización conocida, tecnología, o servicio Pero los riesgos que encuentran son comúnmente vistos y manejados por muchos tipos de organizaciones. Los materiales de ejemplo relacionados con la organización de ejemplo se proporcionan en el documento *CIS_RAM_Workbook* en plantillas reutilizables.

El lector desarrollará mejor la comprensión del método de evaluación de riesgos siguiendo junto con el libro de trabajo, y al ingresar sus propios ejemplos en los espacios provistos dentro de cada hoja de trabajo de muestra.

Pagina 12

Centro de seguridad de Internet ®

Método de evaluación de riesgos

CIS RAM Versión 1.0

Abril 2018

Capítulo 1: Manual de análisis de riesgos

RAM de la CIA describe un método para el análisis de riesgos de ciberseguridad que incluye métodos que son nuevos para la mayoría de los lectores. El Capítulo 1 proporcionará una explicación y descripción de nuevos conceptos, lenguaje y procesos para proporcionar al lector una base sólida para los capítulos restantes.

Después de completar el Capítulo 1, el lector será dirigido a uno de los tres capítulos que proporcionan instrucciones para realizar evaluaciones de riesgos. Los capítulos 2, 3 y 4 presentan procesos, materiales, y ejemplos que son adecuados para organizaciones con diversos grados de capacidad para realizar evaluaciones de riesgo.

Después de completar los capítulos de instrucciones, todos los lectores se beneficiarán de la orientación, consejos y inmersiones profundas presentadas en el Capítulo 5.

Página 14

Método de evaluación de riesgos CIS para el debido cuidado

Introducción

Las leyes, regulaciones y estándares de seguridad de la información no esperan que el público pueda o quiera prevenir todos los incidentes de seguridad de la información. En su lugar, nos hacen responsables de mirar hacia el futuro qué podría salir mal, y usar salvaguardas que no sean demasiado pesadas para evitar eso daño. Esa es la esencia de Duty of Care Risk Analysis [4] ("DoCRA") en el que se basa la RAM CIS en.

- Desde 1993, todas las regulaciones de los EE. UU., Estén o no relacionadas con la información seguridad: requiere un análisis de riesgos para lograr un equilibrio costo-beneficio mientras se logra conformidad. [5] [5]
- Los estándares de seguridad de la información han pedido al público que utilice el análisis de riesgos cuando

diseñando controles de seguridad que coincidan con su entorno. [6][6]

- Los jueces han utilizado una "prueba de equilibrio del deber de cuidado" para determinar la responsabilidad en la violación de datos casos. [7][7]
- La Comisión Federal de Comercio siempre ha requerido que las organizaciones usen el riesgo evaluaciones para determinar la razonabilidad de sus controles de seguridad. [8]
- El Reglamento General de Protección de Datos ("GDPR") que requiere protecciones de privacidad para los residentes de la UE, y basa sus requisitos de seguridad en el análisis de riesgos. [9][9]

Los expertos y las autoridades requieren constantemente que las organizaciones aseguren la información y los sistemas a medida que tanto como puedan para evitar daños a otros, pero no para permitir que las salvaguardas sean demasiado pesadas a ellos o al público. Y señalan las evaluaciones de riesgos como la forma de encontrar el equilibrio.

[4] También conocido como DoCRA Standard. https://www.docra.org.

[5] La Orden Ejecutiva 12866 ”firmada en 1993 requiere que todas las regulaciones federales se apliquen utilizando Análisis de beneficios. La Oficina de Administración y Presupuesto hace cumplir el pedido en parte al exigir que las organizaciones reguladas utilizan evaluaciones de riesgos para identificar controles efectivos que son "razonable."

[6] Ver ISO / IEC 27001: 2013, NIST SP 800-53 Rev. 4, PCI-DSS v3.2

[7] Ver *Dittman v. UPMC* , 154 A.3d 318 (Pa. Super. Ct. 2017), *In re: Cliente de Target Corporation Litigio de incumplimiento de seguridad de datos* , *Memorando y orden,* MDL No. 14-2522 (D. Minn. 2014)

[8] Comisión Federal de Comercio. "Declaración de la Comisión que marca la seguridad de datos número 50 de la FTC Liquidación ". Www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf

[9] Reglamento general de protección de datos. Directiva 95/46 / CE.

Página 15

Bases en Derecho y Regulación

El método de análisis de riesgos de CIS RAM fue diseñado para proporcionar un terreno común para los especialistas en seguridad y gerentes de negocios, y para las autoridades legales y reguladoras que deben evaluar el Suficiencia de salvaguardas de seguridad.

El análisis de riesgos se convirtió en la base de la ley reguladora en 1993 cuando el presidente Bill Clinton firmó un orden ejecutiva, EO 12866, [10] que requería que las regulaciones se hicieran cumplir utilizando un costo-beneficio análisis. La Oficina de Administración y Presupuesto determinó que la mejor manera de lograr costos El análisis de beneficios consistía en incorporar el análisis de riesgos en todas las regulaciones existentes y nuevas.

A partir de 1999, Estados Unidos comenzó a hacer cumplir las regulaciones con seguridad de la información y requisitos de privacidad que utilizan el análisis de riesgos como base para el cumplimiento. El Gramm-Leach-Regla de salvaguardias de la Ley Bliley, [11] la Regla de seguridad de HIPAA, [12] y la Comisión Federal de Comercio requiere que las organizaciones realicen evaluaciones de riesgos para definir sus propios objetivos de cumplimiento. Riesgo las evaluaciones deberían ayudar a las organizaciones a determinar por sí mismas la probabilidad y el impacto de amenazas que podrían dañar al público y garantizar que las salvaguardas no sean excesivamente gravosas. Este análisis de riesgos se ha descrito comúnmente como "Riesgo = Impacto x Probabilidad".

Alrededor de este tiempo, esta misma idea surgió de forma independiente entre un conjunto separado de profesionales. Los organismos nacionales e internacionales de seguridad de la información elaboraron una evaluación de riesgos. métodos como las publicaciones especiales NIST 800-30, ISO 27005 y RISK IT para ayudar al público evaluar riesgos en entornos de tecnología de la información. Estas normas de seguridad de la información también utilizó la misma ecuación utilizada por los reguladores de EE. UU. - "Riesgo = Impacto x Probabilidad" - para expresar la

previsibilidad del daño que puede llegar a la información y los sistemas de información.

Paralelamente al desarrollo de estos dos esfuerzos (y desde principios del siglo XX) abogados y jueces debatieron en salas de tribunales y en revistas de derecho sobre cómo determinar si alguien actuó como una "persona razonable" cuando un demandante demandó por daños y perjuicios. Estos debates llevaron a la creación de la "Regla de la mano aprendida" [13] (también conocido como "el cálculo de la negligencia"). La regla de la mano, como ahora se sabe, establece que una **carga** para prevenir daños no debe ser mayor que la **probabilidad** de daño multiplicada por la **responsabilidad** después de un evento dañino; o matemáticamente establecido, B <= P x L. Los tribunales (de forma variable) han extendido esta regla a las "pruebas de equilibrio del deber de cuidado" que determinan si la falta de previsión y las salvaguardas menos que razonables provocaron daños.

Pero mientras estas disciplinas - ley, seguridad de la información y regulaciones - todas se basaron en un común definición de riesgo, cada uno parecía desconocer los métodos de análisis de riesgo del otro. Aun así, cada la disciplina buscó un traductor universal que permitiera a toda la comunidad de expertos y autoridades para entenderse.

El CIS RAM proporciona ese traductor universal.

[10] *Orden ejecutiva 12866 - Planificación y revisión reglamentaria* , 58 FR 51735; 4 de octubre de 1993

[11] Ley Gramm Leach Bliley Ley de Salvaguardias Regla 16 CFR Parte 314

[12] Regla de Seguridad HIPAA 45 CFR Parte 160 y Subparte A y C de la Parte 164

[13] *US v. Carroll Towing* , 159 F.2d 169 (2d Cir. 1947)

Página 16

Principios y prácticas de CIS RAM

CIS RAM adopta los tres principios y diez prácticas del Análisis de Riesgo del Deber de Cuidados. los tres principios establecen las características de las evaluaciones de riesgos que se alinean con las normativas y legales esperanzas de heredar. Las diez prácticas describen características de las evaluaciones de riesgos que hacen que las tres principios alcanzables.

Principios

1. El análisis de riesgos debe considerar los intereses de todas las partes que puedan verse perjudicadas por el riesgo.
2. Los riesgos deben reducirse a un nivel que las autoridades y las partes potencialmente afectadas encontrar apropiado
3. Las salvaguardas no deben ser más onerosas que los riesgos contra los que protegen.

Practicas

1. El análisis de riesgos considera la probabilidad de que ciertas amenazas puedan crear magnitudes de impacto.
2. Los riesgos y las salvaguardas se evalúan utilizando los mismos criterios para poder compararlos.
3. Los puntajes de impacto y probabilidad tienen un componente cualitativo que establece concisamente preocupaciones de las partes interesadas, las autoridades y la organización evaluadora.
4. Los puntajes de impacto y probabilidad se derivan de un cálculo numérico que permite comparabilidad entre todos los riesgos evaluados, salvaguardas y criterios de aceptación de riesgos.
5. Las definiciones de impacto aseguran que la magnitud del daño a una de las partes se equipare con el magnitud del daño a los demás.
6. Las definiciones de impacto deben tener un límite explícito entre esas magnitudes que sería aceptable para todas las partes y las que no lo serían.
7. Dirección de definiciones de impacto; La misión o utilidad de la organización para explicar por qué la organización y otros involucran el riesgo, los objetivos egoístas de la organización y el Obligaciones de la organización de proteger a otros de daños.

8. El análisis de riesgos se basa en un estándar de atención para analizar los controles actuales y recomendados salvaguardas
9. El riesgo es analizado por expertos en la materia que usan evidencia para evaluar riesgos y salvaguardas
10. Las evaluaciones de riesgos no pueden evaluar todos los riesgos previsibles. Las evaluaciones de riesgo vuelven a ocurrir Identificar y abordar más riesgos con el tiempo.

Página 17

La Tabla 1 alinea estos principios y prácticas con las tres disciplinas de ley, regulaciones y normas de seguridad de la información.

Tabla 1 - Alineación de principios y prácticas de RAM de CIS a la ley, regulaciones y estándares de seguridad

Principios y prácticas de CIS RAM y DoCRA	Ley	Reglamento	Seguridad Normas
El análisis de riesgos debe considerar los intereses de todas las partes. eso puede verse perjudicado por el riesgo.			
Los riesgos deben reducirse a un nivel que las autoridades y las partes potencialmente afectadas encontrarían apropiado.			
Las salvaguardas no deben ser más gravosas que los riesgos. protegen contra.			
El análisis de riesgos considera la probabilidad de que ciertas amenazas podría crear magnitudes de impacto.			
Los riesgos y las salvaguardas se evalúan utilizando el mismo criterios para que puedan ser comparados.			
Los puntajes de impacto y probabilidad tienen una cualitativa componente que expone de manera concisa las preocupaciones de partes interesadas, autoridades y la evaluación organización.			
Los puntajes de impacto y probabilidad se derivan de un valor numérico cálculo que permite la comparabilidad entre todos los evaluados riesgos, salvaguardas y criterios de aceptación de riesgos.			
Las definiciones de impacto aseguran que la magnitud del daño a una parte se equipara con la magnitud del daño a otros.			
Las definiciones de impacto deben tener un límite explícito entre esas magnitudes que serían aceptables para todas las partes y las que no serían			
Dirección de definiciones de impacto; la misión de la organización o utilidad para explicar por qué la organización y otros participan riesgo, los objetivos egoístas de la organización y el Obligaciones de la organización de proteger a otros de daños.			
El análisis de riesgos se basa en un estándar de atención para analizar controles actuales y salvaguardas recomendadas.			
El riesgo es analizado por expertos en la materia que utilizan evidencia para evaluar riesgos y salvaguardas.			

Las evaluaciones de riesgos no pueden evaluar todos los riesgos previsibles.
Las evaluaciones de riesgos vuelven a ocurrir para identificar y abordar más riesgos con el tiempo.

Clave : Completamente dirigido Parcialmente dirigido No abordado

Las organizaciones que realizan evaluaciones de riesgos utilizando la RAM CIS tendrán un plan para implementando los Controles CIS V7 que sean razonables y defendibles tanto para las autoridades como para los expertos.

Página 18

Evolución de los métodos de análisis de riesgos

Evolución de los conceptos de riesgo clásicos
Para unir el análisis de riesgos de seguridad de la información con las expectativas legales y regulatorias, CIS RAM se basa y extiende algunos conceptos clásicos de análisis de riesgos. Esta sección describirá brevemente cómo CIS RAM desarrolla la evaluación de riesgos y las definiciones de "impacto", aceptación de riesgos y riesgo residual.

Calcular el riesgo incluye múltiples impactos
CIS RAM utiliza el clásico cálculo de evaluación de riesgos "Riesgo = Impacto x Probabilidad" con algunas modificaciones Más significativamente, el riesgo se calcula multiplicando un valor de probabilidad por múltiples valores de impacto. Estos impactos múltiples incluyen impactos a los objetivos de la organización, es misión, y es la obligación de proteger a los demás. Las organizaciones deben ser conscientes de las muchas formas ese riesgo de seguridad de la información puede crear daño.

El cálculo de riesgo utilizado por CIS RAM se asemeja a la estructura a continuación:
"Riesgo = Máx. (Impacto de misión, Impacto de objetivos, Impacto de obligaciones) x Probabilidad".

Las instrucciones proporcionadas más adelante en este documento describen claramente cómo funciona este cálculo. Las organizaciones que usan este cálculo extendido considerarán constantemente las muchas formas en que Los riesgos de seguridad de la información pueden crear daños.

Las definiciones de impacto incluyen daños a múltiples partes
Para garantizar la equidad y el equilibrio, las definiciones de impacto incluirán posibles daños a las personas y organizaciones que pueden verse afectadas por los riesgos. Los impactos y las magnitudes de impacto se expondrán en forma cualitativa y cuantitativa para comunicar fácilmente los niveles de riesgo a todas las partes interesadas, y de una manera que le importa a cada parte.

La aceptación del riesgo está claramente definida
CIS RAM proporciona a las organizaciones una guía clara para definir un riesgo aceptable que parezca justo a las autoridades y partes interesadas, y eso se puede aplicar de manera consistente a toda la información riesgos de seguridad.

El riesgo aceptable considerará si un riesgo observado es "apropiado" (todos potencialmente afectados las partes estarían de acuerdo en que el riesgo es aceptable) y si una salvaguarda recomendada es “Razonable” (no crea más carga que el riesgo contra el que protege).

Al ampliar la definición de aceptación del riesgo por estos dos factores, las organizaciones tendrán una justificación fácilmente comunicada para aceptar riesgos o para priorizar riesgos inaceptables.

El "riesgo residual" se conoce como "riesgo de salvaguardia"
"Riesgo residual" ha significado tradicionalmente la cantidad reducida de riesgo que queda después de una seguridad El control ha sido implementado. Las organizaciones generalmente han usado "residual" para declarar cómo La protección de seguridad planificada presenta un riesgo aceptable. CIS RAM evoluciona la noción de un "residual riesgo ”para“ salvaguardar el riesgo ”para describir el riesgo que puede presentar una nueva salvaguarda.

El propósito de evaluar el riesgo residual de esta manera es abordar el hecho de que los nuevos controles a menudo

tener consecuencias no deseadas Recuerde que las definiciones de impacto se basarán en múltiples factores, como la misión de una organización, sus objetivos y sus obligaciones (descritas con más detalle más adelante en el documento). Los controles de seguridad pueden reducir el riesgo para las obligaciones de seguridad al controlar acceso a datos, pero puede aumentar el riesgo para la misión de la organización que requiere compartir el datos. Las decisiones y regulaciones legales consideran estas salvaguardas excesivas como "cargas" porque pueden dañar a la organización que está tratando de proteger los datos.

Página 19

Al evaluar el riesgo de salvaguarda utilizando los mismos criterios que se utilizan para evaluar los riesgos, las organizaciones será más consciente del verdadero costo de los controles y tendrá una forma defendible de declarar si los controles recomendados son demasiado gravosos para ellos o para el público.

Aceptabilidad del riesgo en evolución

La Figura 1 ilustra cómo CIS RAM evalúa el riesgo "apropiado" utilizando una declaración de riesgo simplificada. En En este escenario, una organización está analizando el riesgo de pérdida de un dispositivo y estima la probabilidad y Impacto esperado de la pérdida. Las definiciones de impacto estiman el daño potencial a la organización y a otros.

Usando una escala de '1' a '3', la organización multiplica el puntaje de probabilidad por el más alto de los dos puntajes de impacto para llegar a un puntaje de riesgo de '6'. En este ejemplo, un riesgo aceptable sería menor que '4', entonces el puntaje de '6' no es apropiado. "Otros" no aceptarían la posibilidad de este riesgo.

Nota: La RAM de CIS proporciona una amplia guía sobre cómo la puntuación de probabilidad e impacto y Se definen criterios de riesgo aceptables. Los valores de la Figura 1 y la Figura 2 se proporcionan simplemente para fines ilustrativos

Figura 1 - Modelo de riesgo simplificado que muestra riesgo inapropiado

En la Figura 2, el riesgo excesivamente alto se corresponde con una protección recomendada para cifrar todo dispositivos. Debido a que una salvaguarda se evalúa utilizando los mismos criterios que el riesgo, la organización es evaluando la carga de la salvaguardia. En este caso, creen que hay una pequeña probabilidad ('1') de un notable impacto en los costos ('2'). Como resultado, el riesgo de salvaguardia se calcula como '2', que es menor que el riesgo observado que está abordando ('6'). Como resultado, esta salvaguarda es razonable.

Figura 2 - Modelo de riesgo simplificado que muestra una salvaguarda razonable

Página 20

¿Vale la pena este análisis extendido?
En pocas palabras, sí.

Los controles de seguridad de la información a menudo se consideran un obstáculo para los negocios. Los usuarios a menudo quejarse de que los controles de seguridad obstaculizan la productividad, la eficiencia, la facilidad de colaboración y comunicación y otras preocupaciones que afectan el negocio. Las organizaciones deberían tomar estos Quejas en serio. Afortunadamente, los reguladores han proporcionado a las organizaciones un medio para evaluar estas preocupaciones Además, los tribunales consideran la carga de las salvaguardas en los juicios y entendería el razonamiento que proporciona este análisis de riesgos.

Al evaluar los riesgos y sus salvaguardas recomendadas utilizando el mismo criterio, las organizaciones Asegurar que el análisis de riesgos aborde las preocupaciones de todas las partes dentro y fuera de su organización, y proporciona evidencia de su decisión concienzuda a los reguladores y jueces.

Descripción general del método de evaluación de riesgos CIS

Uso de evaluaciones de riesgos para diseñar y evaluar controles CIS V7
CIS Controls V7 fue diseñado para abordar las causas más comunes de incidentes de seguridad en el público en general. Como resultado, los Controles CIS tienen un grado de prioridad de riesgo, especialmente si Las organizaciones implementan los primeros cinco controles CIS antes de implementar los 15 restantes. Sin embargo, cada organización tiene circunstancias especiales, incluido el daño potencial que pueden causar. causar a otros, la necesidad de operar sistemas algo vulnerables basados en su misión, la necesidades de sus constituyentes, sus recursos disponibles y la previsibilidad de las amenazas en sus industria.

El método de evaluación de riesgos descrito por CIS RAM ayudará a las organizaciones a determinar si su implementación de CIS Controls V7 - o su des-priorización o personalización de controles - es Consideraciones de seguridad, legales y regulatorias razonables y apropiadas.

Este método de evaluación de riesgos describe múltiples formas en que las organizaciones pueden evaluar, evaluar, y diseñar salvaguardas utilizando los controles CIS.

- En algunos casos, las organizaciones pueden comenzar simplemente y enumerar los controles para determinar si sus activos de información son lo suficientemente resistentes contra las amenazas previsibles.
- Las organizaciones más capaces pueden enumerar primero sus activos de información, luego considerar si Los controles CIS asociados protegen suficientemente esos activos contra las amenazas previsibles.
- Las organizaciones con un comando de cómo operan las amenazas pueden comenzar con una lista de amenazas previsibles contra los activos de información y determinar cómo deben ser los controles implementado para abordarlos.

Cada uno de estos enfoques se basa en la capacidad de la organización para realizar ese tipo de análisis. Y esas habilidades dependen de la participación de la gestión empresarial en la seguridad de la información, el disponibilidad de tiempo y recursos para examinar los activos y riesgos de la información, y la experiencia de El personal para realizar el análisis.

En cualquier caso, este método de evaluación de riesgos proporcionará un modelo para que las organizaciones evalúen los riesgos. con base en el daño que pueden plantearse a sí mismos o a sus electores, y para determinar si la carga de cada uno de los controles de la CEI, implementados como salvaguardas, es apropiada.

Proceso de evaluación de riesgos
Una evaluación de riesgos es un proyecto que analiza el riesgo planteado por un conjunto de activos de información, y recomienda salvaguardas para abordar riesgos inaceptablemente altos.

Si bien el orden de los eventos en un proyecto de evaluación de riesgos variará de una organización a otra, En general, se aplican las siguientes actividades:

Página 21

Analizar el riesgo observado

- Definir el alcance: identificar los activos de información que se están evaluando, así como los propietarios y administradores de los activos de información.
- Programar sesiones: programe las entrevistas y sesiones para la revisión de la evidencia.
- Desarrollar la evaluación de riesgos y los criterios de aceptación: establecer y definir los criterios para evaluando y aceptando riesgos.
- Recopilar evidencia: entrevistar al personal, revisar documentos y observar salvaguardas.
- Modele los riesgos: evalúe las salvaguardas actuales que evitarían o detectarían previsibles amenazas contra la seguridad de los activos de información.
- Evaluación de riesgos: calcule la probabilidad y el impacto de las infracciones de seguridad para calcular el riesgo puntuación, luego determine si los riesgos identificados son aceptables.

Proponer salvaguardias

- Proponer salvaguardas: recomendar salvaguardas de los Controles CIS V7 que reducirían riesgos inaceptables
- Evaluar las salvaguardas propuestas: analizar el riesgo de las salvaguardas recomendadas para asegurar que plantean riesgos aceptablemente bajos sin crear una carga indebida.

Criterios de evaluación de riesgos

El análisis de riesgos requiere un método consistente y repetible para estimar y evaluar el riesgo. Riesgo Los criterios de evaluación brindan a las organizaciones medidas para calificar consistentemente la probabilidad y impacto de las amenazas previsibles que pueden comprometer la seguridad de los activos de información.

Los criterios de evaluación de riesgos a menudo se consideran en términos de una cuadrícula de 3 x 3 o una cuadrícula de 5 x 5, con cada dimensión que representa valores de "probabilidad" o valores de "impacto". Mientras que las puntuaciones de '1' a través '3' o '1' aunque '5' son convenientes para calcular el riesgo como producto, no son significativos por sí mismos. Por lo tanto, los criterios también deben tener un componente en lenguaje sencillo que describa los niveles de impacto y probabilidad que son significativos para la organización.

Los criterios de evaluación de riesgos en un formato simplificado pueden parecer similares a esto:

Tabla 2 - Criterios de impacto simplificados

Puntaje de impacto	Puntaje de impacto definido
1	No se producirá daño mínimo o mínimo.
2	El daño no sería tolerable.
3	El daño puede no ser recuperable.

Tabla 3 - Criterios de probabilidad simplificados

Puntuación de probabilidad	Puntuación de probabilidad definida
1	No previsible
2	Se espera que ocurra.
3	Ocurrencia regular.

Página 22

Criterios de aceptación de riesgos

Las leyes y regulaciones requieren que las organizaciones apliquen salvaguardas "razonables" y "apropiadas" para garantizar que el riesgo resultante sea aceptable. La aceptabilidad del riesgo puede demostrarse utilizando

análisis de riesgos que aborde la tolerabilidad del riesgo y la carga de las salvaguardas que protegen contra el riesgo

Si bien cada organización definirá su propia tolerancia al riesgo, este método proporciona un proceso para hacerlo usando lenguaje simple y matemática simple. Un ejemplo de definición de aceptabilidad del riesgo es proporcionado en la Tabla 4 utilizando los criterios simplificados de impacto y probabilidad de arriba. Organizaciones desarrollará sus criterios de aceptación de riesgos definiendo primero qué es el riesgo inaceptable.

En este caso, la organización ha determinado sus criterios de aceptación de riesgos al decidir primero que No acepte un riesgo que pueda causar un daño intolerable (como lo indica el cuadro rojo).

Tabla 4 - Criterios de impacto simplificados para la aceptación del riesgo

Puntaje de impacto	Nivel de impacto	Puntaje de impacto definido
1	Aceptable	No se producirá daño mínimo o mínimo.
2	Inaceptable	El daño no sería tolerable.
3	Alto	El daño puede no ser recuperable.

Luego, la organización determinó que se espera que ocurra una amenaza (y que genere daño) debe evitarse (como se indica en el cuadro rojo en la Tabla 5).

Tabla 5 - Criterios de probabilidad simplificados para la aceptación del riesgo

Puntuación de probabilidad	Puntuación de probabilidad definida
1	No se espera que ocurra
2	Se espera que ocurra
3	Ocurrencia regular

Y finalmente, la organización combinó estos límites para expresar su riesgo aceptable en ambos lenguaje, y en términos matemáticos.

Tabla 6 - Criterios de aceptación de riesgos

Versión	Definiciones de riesgo aceptable
Lenguaje simple	Debemos reducir los riesgos que se espera que generen daños intolerables.
Matemático	Riesgo aceptable <2 x 2; o riesgo aceptable <4

Página 23

Antecedentes: "razonabilidad" y análisis de riesgos

La "persona razonable" se usa en la ley como una persona hipotética - o ficción legal - que encarna la suma de nuestras tradiciones, valores y responsabilidades para cuidar de no dañar otros mientras nos involucramos en la vida pública. La persona razonable ha sido utilizada en casos para evaluar el comportamiento apropiado para actividades tales como construir y mantener estructuras, ofreciendo bienes y servicios, o manejando activos como información e información tecnologías Una persona razonable puede participar en actividades para su propio beneficio, pero debe tomar cuidado, usando las precauciones apropiadas, para no dañar a otros en el proceso.

En un litigio, un juez a menudo utilizará una prueba de equilibrio de "deber de cuidado" o "factor múltiple" para determinar el grado en que un acusado estaba actuando razonablemente cuando un demandante fue dañado. Y en

Las organizaciones reguladoras deben aplicar salvaguardas “razonables” para proteger a otros de daños. La prueba de equilibrio del deber de cuidado del juez es muy similar en estructura a esta evaluación de riesgos método. Una organización considerará las amenazas previsibles que su negocio puede causar. otros. Determinarán qué tan efectivamente previenen ese daño al usar los Controles CIS V7 como estándar para las prácticas apropiadas de seguridad cibernética. Ellos estimarán la probabilidad y impacto del daño esperado de una amenaza previsible, y considerarán alternativas salvaguardas que efectivamente reducen los riesgos sin ser excesivamente gravosas. De esta manera, los jueces y los profesionales de ciberseguridad usan el mismo lenguaje para describir la ciberseguridad razonable prácticas

De manera similar, un regulador pedirá a las organizaciones reguladas que demuestren razonabilidad de sus salvaguardas revisando el registro de riesgos de la organización. Desde 1993 Las regulaciones federales de los Estados Unidos requieren que las reglas regulatorias no sean excesivamente gravosas para el público, y que se realiza un análisis de "costo-beneficio" para determinar si las acciones regulatorias son demasiado pesado y apropiado para proteger al público. Agencias reguladoras, incluidas aquellas que rigen las normas y reglamentos de ciberseguridad, requieren evaluaciones de riesgos como método para equilibrar el daño potencial a otros con el costo de las salvaguardas.

Selección de un nivel para sus instrucciones de evaluación de riesgos

Este documento está diseñado para ser útil para organizaciones con diferentes niveles de seguridad. capacidades de gestión. Estos niveles de capacidad se alinean con los niveles de implementación del marco ("Niveles") según lo definido por el Marco de Ciberseguridad NIST. [14] Los niveles indican "cómo un organización ve riesgos de seguridad cibernética y los procesos para gestionar ese riesgo.” [15] Los Niveles están definidos por NIST de la siguiente manera (abreviada).

Nivel 1: Parcial

- *Proceso de gestión de riesgos* : informal y ad hoc.
- *Programa integrado de gestión de riesgos* : conciencia limitada dentro de la organización.
- *Participación externa* : no se coordina con entidades externas.

[14] *Marco para Mejorar la Ciberseguridad de Infraestructura Crítica, Versión 1.0* , Instituto Nacional de Estándares y tecnología. 12 de Febrero de 2014

[15] Ibid, pág. 9)

Página 24

Nivel 2: Riesgo informado

- *Proceso de gestión de riesgos* : informado por los objetivos de riesgo de la organización.
- *Programa integrado de gestión de* riesgos: informado sobre riesgos, aprobado por la gerencia procesos y procedimientos.
- *Participación externa* : no se coordina con entidades externas.

Nivel 3: Repetible

- *Proceso de gestión de riesgos* : aplicado a través de políticas y actualizado con cambios en el medio ambiente y amenazas.
- *Programa integrado de gestión de* riesgos: se utilizan políticas y procesos informados sobre riesgos En toda la empresa. El personal está capacitado e informado para trabajar de manera segura.
- *Participación externa* : recepción de información de los socios para realizar un análisis interno basado en el riesgo. decisiones

Nivel 4: Adaptativo

- *Proceso de gestión de riesgos* : adaptable a través de las lecciones aprendidas y continuo

mejora.

- *Programa integrado de gestión de riesgos* : cultura de conciencia de seguridad en toda la empresa y mejora continua basada en lecciones aprendidas e información externa.
- *Participación externa* : compartir información de seguridad y amenazas con los socios.

CIS RAM proporciona tres conjuntos de instrucciones, plantillas, ejercicios y ejemplos para realizar evaluaciones de riesgo, cada una con una complejidad creciente. Estos tres conjuntos de materiales son adecuados para Organizaciones de nivel 1, organizaciones de nivel 2 y organizaciones de nivel 3 y nivel 4. El lector puede determinar cuál de estos niveles y documentación son los más adecuados para ellos mediante la revisión de características proporcionadas a continuación.

Los materiales de **nivel 1** son adecuados para organizaciones con las siguientes características:

- **Nivel NIST** : organizaciones de Nivel 1. Los materiales de nivel 1 son los más adecuados para organizaciones que lo hacen no coordinar sus planes y requisitos de seguridad de la información en todo el organización. La seguridad de la información está impulsada en gran medida por la gestión de la tecnología.
- **Experiencia** : la organización puede identificar amenazas genéricas, pero no métodos específicos. para hackear sistemas, dispositivos y aplicaciones.
- **Tiempo** : la organización puede absorber el tiempo necesario para evaluar los riesgos de información en el nivel de sistemas genéricos, dispositivos y aplicaciones.

Los materiales de **nivel 2** son adecuados para organizaciones que disfrutan de una mayor colaboración con las empresas. gestión y tener más recursos y capacidades para analizar los riesgos de seguridad y la planificación programas

- **Nivel NIST** : organizaciones de Nivel 2. Los materiales de nivel 2 son los más adecuados para organizaciones que tener al menos alguna colaboración con la gerencia comercial no técnica para definir el riesgo criterios
- **Experiencia** : la organización tiene recursos y capacidades para analizar la seguridad común amenazas y planificar salvaguardas apropiadas para el riesgo. Sin embargo, no tienen a la mano habilidades para modelar cómo operarían las amenazas dentro de su organización.

Página 25

- **Tiempo** : la organización puede invertir suficiente tiempo para analizar los riesgos a nivel de sistemas, dispositivos y aplicaciones específicos, y subcomponentes dentro de esos activos.

Los materiales de nivel 3 o 4 son adecuados para organizaciones que reciben información de seguridad y amenazas de fuentes externas, que tienen un conocimiento significativo de los temas de seguridad de la información y tiempo para evaluar escenarios de amenazas en los que se basan las evaluaciones de riesgos.

- **Nivel NIST** : organizaciones de niveles 3 y 4. Los niveles 3 o 4 son los más adecuados para organizaciones que utilizan criterios basados en el riesgo para políticas de toda la empresa y procesos.
- **Experiencia** : la organización tiene recursos y capacidades para analizar amenazas de seguridad, y planificar salvaguardas apropiadas para el riesgo, incluidas las habilidades disponibles para modelar cómo las amenazas operaría dentro de su organización.
- **Tiempo** : la organización puede invertir tiempo para analizar los riesgos a nivel específico. sistemas, dispositivos y aplicaciones en el contexto de amenazas específicas.

El lector debe determinar qué materiales de nivel son los más adecuados para su organización, y debe seguir las instrucciones que se proporcionan en ese nivel. También pueden decidir aprender y usar los métodos descritos en otros conjuntos de instrucciones, pero deben permanecer dentro de su nivel tanto como posible hasta que se sientan cómodos con sus procesos de evaluación de riesgos existentes.

Capítulo 2: Evaluación de riesgos basada en el control Instrucciones para organizaciones de nivel 1

Las instrucciones de evaluación de riesgos del **Nivel 1** son adecuadas para organizaciones que se ajustan al perfil del Nivel 1 organizaciones según lo descrito por el NIST Cybersecurity Framework **.** Estas organizaciones pueden ser identificado por tener las siguientes características:

- **Nivel NIST** : organizaciones de Nivel 1. Los materiales de nivel 1 son los más adecuados para organizaciones que lo hacen no coordinar sus planes y requisitos de seguridad de la información en todo el organización. La seguridad de la información está impulsada en gran medida por la gestión de la tecnología.
- **Experiencia** : la organización puede identificar amenazas genéricas, pero no métodos específicos. para hackear sistemas, dispositivos y aplicaciones.
- **Tiempo** : la organización puede absorber el tiempo necesario para evaluar los riesgos de información en el nivel de sistemas genéricos, dispositivos y aplicaciones.

Este capítulo consta de secciones que abordan cada una de las actividades específicas dentro de un riesgo. evaluación. Los lectores deben participar en este capítulo leyendo primero el texto en cada sección, y luego realizar los ejercicios que se recomiendan para cada sección. El material presentado en la RAM CIS es sustancialmente diferente de muchos otros estándares y modelos de evaluación de riesgos, así que el lector primero debe comprender el objetivo de cada sección y luego practicar lo que aprende utilizando plantillas que se proporcionan en el documento complementario *CIS_RAM_Workbook* .

Al realizar su primera evaluación de riesgos basada en RAM CIS, las organizaciones deben tener cuidado de no trate de "hervir el océano". Los organismos reguladores y las normas de seguridad de la información entienden por igual que no todos los riesgos pueden identificarse en una sola evaluación. Las organizaciones deben continuamente y Evaluar regularmente los riesgos para identificar, comprender y gestionar los riesgos a lo largo del tiempo.

El proyecto de evaluación de riesgos

Visión general

Las evaluaciones de riesgos son proyectos con pasos claros para preparar, conducir y reportar riesgos

análisis. Y aunque los proyectos de evaluación de riesgos se pueden modelar con un plan típico, cada
El enfoque del proyecto de la organización variará dependiendo de factores como la disponibilidad de recursos y
se desarrollará con el tiempo a medida que las organizaciones se vuelvan más capaces en su madurez de ciberseguridad. Esta
La sección describirá un proyecto de evaluación de riesgos, sus componentes y variaciones, y presentará
orientación para preparar el plan.

El esquema del proyecto
Las evaluaciones de riesgos se realizan utilizando una serie de pasos que incluyen acciones típicas y roles como
ilustrado en la Tabla 7.

Tabla 7 - Ejemplo de esquema de proyecto de evaluación de riesgos

Paso	Tarea	Papeles clave
1	Definición del alcance y la programación de sesiones	Ejecutivos, Gerencia, Asesor
2	Definición de criterios de evaluación de riesgos	Gerente, Asesor
3	Definición de criterios de aceptación de riesgos	Ejecutivos, Gerencia, Asesor

Página 27

Paso	Tarea	Papeles clave
4 4	Evaluación de riesgos (basada en control)	
4.1	Reunir evidencias	Personal, Gerencia, Asesor
4.2 4.2	Modelar las amenazas	Personal, Gerencia, Asesor
4.3 4.3	Evaluación de riesgo	Asesor
5 5	Proponer salvaguardias	
5.1	Evaluar las salvaguardas propuestas	Asesor, Gerencia

Durante el **Paso 1** (Definición del alcance y las sesiones de programación), la organización determinará qué
activos de información para incluir en su evaluación. También identificarán dueños de negocios y
delegados técnicos que proporcionarán pruebas y entrevistas para evaluar esos activos. El riesgo
El asesor luego programará sesiones de entrevistas con esos propietarios y delegados.

En el **Paso 2** (Definición de criterios de evaluación de riesgos), la organización definirá las reglas mediante las cuales
evaluar y puntuar riesgos. Definirán su misión (el valor que aportan a los demás) y su
obligaciones (el potencial de daño contra otros) para establecer lo que están tratando de proteger.
Luego definirán los esquemas de puntuación que se utilizarán para el impacto y la estimación de probabilidad.

En el **Paso 3** (Definición de criterios de aceptación de riesgos) la organización establecerá su tolerancia al riesgo mediante
seleccionando una combinación la probabilidad de un impacto que sería tolerable para todas las partes (el
organización y partes que pueden verse perjudicadas por los riesgos realizados).

En el **Paso 4** (Evaluación de riesgos - Basada en el control) el evaluador de riesgos evaluará los riesgos de
activos de información. Para las organizaciones de nivel 1, el análisis incluye las siguientes actividades:

- “Recopilar evidencia” implica una revisión de documentos, como políticas, procedimientos,
  normas y puntos de referencia. También incluye entrevistas con la gerencia y el personal.
  La recopilación de evidencia también implica la observación de configuraciones, artefactos, instalaciones, registros,
  y procesos de trabajo para determinar si operan de manera segura o vulnerable.

  Las organizaciones de nivel 1 también deberían considerar revisar las configuraciones de controles y
  buscando evidencia de su efectividad. Esto puede ser un desafío para las organizaciones en
  este nivel. Los escáneres de vulnerabilidad y los escáneres de configuración que utilizan políticas SCAP pueden
  Proporcionar un análisis eficiente de los sistemas técnicos para ayudar en este análisis.

- **“** Modelar las amenazas” implica la mayor variedad de enfoques que dependen de
  Ciberseguridad madurez de la organización. Sin embargo, cada organización modelará los riesgos.
  con al menos estos componentes: teniendo en cuenta los controles CIS que deberían estar en su lugar para
  proteger los activos de información; determinar si esas salvaguardas están efectivamente establecidas
  para proteger los activos de información; Identificar vulnerabilidades que pueden permitir violaciones de
  bienes; e identificar amenazas que podrían aprovechar esas vulnerabilidades.

• Durante la “Evaluación de riesgos”, la organización estimará la probabilidad y el impacto de la riesgos Las estimaciones se basarán en la puntuación y los criterios establecidos en Paso 2. La puntuación de riesgo se calculará automáticamente para determinar si el actual Las implementaciones de los controles CIS ya son razonables.

Durante el **Paso 5** (Proponer salvaguardas), la organización considerará cómo abordar los motivos irrazonables riesgos seleccionando controles CIS que deben implementarse para abordar cada riesgo, y específicamente

Página 28

cómo se implementarán los controles. Estas salvaguardas pueden incluir dispositivos de seguridad, físicos salvaguardas, capacitación, procesos de supervisión u otros métodos. El evaluador de riesgos luego evaluará el razonabilidad de las salvaguardas durante "Evaluar las salvaguardas propuestas". El evaluador de riesgos evaluar las salvaguardas propuestas utilizando los mismos criterios que se usaron para evaluar los riesgos.

Una plantilla de plan de proyecto está disponible en el documento complementario *CIS_RAM_Workbook* .

Definición del alcance y la programación de sesiones

Nota: Para comprender mejor el contenido de este capítulo, el lector primero debe leer cada sección de el capítulo, luego siga los ejercicios recomendados al final de cada sección para obtener conocimiento práctico de los temas de la sección. Se le indicará al lector que use las plantillas que se proporcionan en el documento complementario CIS_RAM_Workbook para intentar sus ejercicios.

Definiendo el Alcance

Las organizaciones deben realizar evaluaciones de riesgos con un alcance de información claramente definido bienes. Un tema único generalmente limita el alcance de los activos, como "activos de información que contienen información confidencial "," el centro de datos "," áreas y tecnologías de práctica de ingeniería que los respaldan "o una división comercial específica.

Si bien es posible seleccionar activos de información no relacionados para una evaluación, o un subconjunto de activos dentro de un alcance mayor: la organización que recibe la evaluación y está haciendo las inversiones y las decisiones de priorización basadas en sus hallazgos serán más cómodas cuando los activos de información están asociados con una entidad comercial o un proceso comercial. De lo contrario, riesgo Los resultados de la evaluación pueden parecer dispersos y no relacionados.

Del mismo modo, al evaluar el riesgo de un conjunto de activos de información, tiene sentido considerar Un conjunto de activos que pueden afectar directamente la seguridad de los demás. Por ejemplo, una evaluación de riesgos que examina un conjunto de aplicaciones que también deben incluir los dispositivos de red que conectan aplicaciones a otros activos y otras redes, así como los procesos que se utilizan para desarrollar y gestionar esas aplicaciones. Estos sistemas están directamente conectados entre sí y dependen unos de otros por lo que sus riesgos se asocian fácilmente entre sí.

Las organizaciones no pueden examinar todos los activos de información de manera integral en un solo riesgo evaluación, por lo que su alcance debe considerar el tiempo y los recursos disponibles para evaluación . Los evaluadores de riesgos deben consultar a expertos en seguridad para ayudarlos a determinar qué activos para priorizar, y puede usar el análisis de riesgo inherente como se describe en el Capítulo 5 para ayudar en esto priorización

Una tabla de alcance de ejemplo (Tabla 8) demuestra el nivel de detalle que puede ser apropiado para un plan de evaluación inicial y se proporciona en el libro de trabajo *CIS_RAM_Workbook*

Tabla 8 - Tabla de alcance de ejemplo

Tipo de activo	Clase de activos	Propietario de la empresa	Mayordomo
Información	IP y PII	ARRULLO	CIO
Solicitud	Aplicaciones	Experiencia del cliente	Prod Mgr, Dev y Dev Ops
Servidores	Servidores	Dev Ops	DevOps
Dispositivo de red	Dispositivos de red	CIO	Ingeniería en Redes
Proceso	Dev, Promoción, Mantenimiento.	Dev Ops	Dev, DevOps
Proceso	Vulnerabilidad Mgt.	CIO	Equipo de seguridad

Proceso	Configuración de cuentas, mantenimiento	Experiencia del cliente	Gestión de aplicaciones

Página 29

Tipo de activo	Clase de activos	Propietario de la empresa	Mayordomo
Proceso	Auditoría interna	Conformidad	Auditoría interna
Proceso	Configuración del dispositivo / sistema	CIO	DevOps
Proceso	Atención al cliente	Experiencia del cliente	Gestión de aplicaciones

Tenga en cuenta que la tabla de alcance incluye roles de propietario de negocio y roles de administrador. Dueños de negocios son los (normalmente) gerentes no técnicos responsables de la información y los procesos que los activos de información de apoyo. Los delegados son (típicamente) gerentes técnicos responsables para la funcionalidad y seguridad de los activos de información. Al identificar el activo de información propiedad por adelantado, la tabla de alcance se puede utilizar para ayudar a planificar sesiones de entrevista para el resto de la evaluación de riesgos.

Independientemente de cómo se establezca el alcance de la evaluación de riesgos y de qué tan detallado sea el activo el listado es, hay algunas prácticas útiles que una organización debe tener en cuenta al identificar sus activos de información:

- Piense en un conjunto de activos ubicados de manera similar como una sola clase de activos. Por ejemplo, todos servidores de bases de datos que usan la misma tecnología y el mismo mantenimiento y Los métodos de administración pueden considerarse una clase de activo. Sin embargo, si un conjunto de los servidores de bases de datos son diferentes de otros (por ejemplo, contienen información confidencial en una DMZ mientras que otros procesan información menos sensible en otra zona), estos pueden ser consideró dos activos porque sus riesgos inherentes serán diferentes, incluso si son gestionado de forma idéntica.
- Los activos de información no son solo tecnologías que almacenan y transmiten información confidencial. Los activos de información son cualquier información, tecnología, proceso, personas o instalaciones que puedan impactar la confidencialidad, integridad o disponibilidad de información.
- Incluir en el alcance todos los activos de información que están dentro de las mismas zonas (redes, instalaciones, etc.) como cualquier otro activo de información dentro del alcance.

Ejercicio :

El lector debe desarrollar su propia tabla de alcance utilizando la hoja de trabajo "Alcance - Nivel 1" que está proporcionado en el documento complementario *CIS_RAM_Workbook* .

El lector debe considerar:

1. Un conjunto de activos de información que su organización está interesada en enfocar su seguridad recursos en?
    a. Este conjunto puede definirse por procesos, tecnologías, una clase de información o una localización.
2. ¿Cuáles son los límites entre este conjunto de activos de información y otra información? activos que no están en este alcance?
    a. Qué sistemas, instalaciones y dispositivos de red vinculan estos límites, o separarlos?
    si. ¿Se incluyen o excluyen estos activos "límite" del alcance?
3. Enumere los activos de información o las clases de activos que están dentro del alcance.
    a. Enumere los activos de información o las clases de activos con un nivel de detalle que el La organización tiene el tiempo y los recursos para analizar. Esto puede requerir ajuste durante el curso de la evaluación si la organización se da cuenta tiene más tiempo (o menos tiempo) de lo que originalmente planearon para evaluar activos de información.

Programación de sesiones de entrevista

Las sesiones de entrevista serán de actualidad y deberán abordar un tema o temas estrechamente relacionados para cada conversacion. Las sesiones de entrevista pueden centrarse en los controles CIS, o en los activos de información y activos clases

Por ejemplo, las sesiones de entrevistas que se centran en los controles de CIS reunirían al personal y gerencia que sabe cómo se implementa y opera cada control. Una sesión puede ser dedicado a CIS Control 1 para comprender cómo se inventarian los dispositivos. Otro puede ser programado para discutir el Control 2 de CIS para comprender qué salvaguardas existen para el inventario software. O, si el mismo personal conoce ambas salvaguardas, entonces quizás una sesión podría combinar ambos temas.

Del mismo modo, si los evaluadores de riesgos programan sesiones en torno a activos de información o clases de activos, entonces sería apropiado incluir dueños de negocios y dueños técnicos de esos sistemas para Comprenda cómo se aplican los controles CIS asociados a cada activo o clase de activo.

Una sesión de ejemplo para una aplicación web puede incluir gerentes de producto, desarrolladores de aplicaciones, administradores de aplicaciones y dueños de negocios. Los temas en esa sesión pueden incluir el Control CIS 14, "Acceso controlado basado en la necesidad de saber", CIS Control 16, "Monitoreo de cuentas y Control "y CIS Control 18," Seguridad del software de aplicación ".

La forma en que la organización agrupa y ordena estos temas depende en gran medida de ellos, pero los evaluadores de riesgos debe tener en cuenta estos consejos al programar sesiones de entrevista:

1. Sea respetuoso con el tiempo de las personas. Si bien es importante recopilar información completa acerca de los riesgos, las organizaciones no pueden recopilar toda la información relevante en el primer o segundo riesgo evaluaciones
2. Trabajar con los gerentes para determinar la forma más eficiente y útil de programar entrevistas, ya sea por CIS Controls o por activos de información y clases de activos.
3. Espere que algunas salvaguardas de seguridad se apliquen de manera diferente a información diferente activos y clases de activos. Por ejemplo, CIS Control 5, "Configuración segura para Hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores "y CIS El control 16, "Monitoreo y control de cuentas" puede implementarse y supervisarse de manera diferente para servidores en diferentes entornos, o puede ser controlado centralmente para servidores, pero controlado individualmente para dispositivos de red. Planee evaluar cómo estos y otros similares Las salvaguardas se aplican a diferentes clases de activos.
4. Proporcione una agenda para la entrevista de alcance para ayudar a los participantes a preparar cualquier material o información sobre los activos o controles de información que pueden discutirse.

Programación de revisiones de evidencia

Los evaluadores de riesgos utilizan sesiones de revisión de evidencia para examinar los activos de información y; determinar si se ajustan a los controles de la CEI y evalúan si serían eficaces contra amenazas previsibles

Las sesiones de revisión de evidencia deben programarse después de las entrevistas para que el riesgo los evaluadores entienden el panorama general del entorno de seguridad antes de intentar Comprenda por qué ciertos activos están configurados de la forma en que están.

Durante las entrevistas, el evaluador de riesgos aprenderá sobre temas que deberían ser más cercanos entendido a través de una revisión de configuraciones, pruebas del sistema o revisión de registros. Evaluadores de riesgos deben tener en cuenta durante o poco después de la entrevista qué garantías querrán examinar más a fondo, e informar a los participantes que probablemente serán contactados más tarde en la evaluación para participar en esas sesiones de revisión de evidencia. Además, el asesor debe preguntar qué personal, procesos o activos de información serían apropiados para examinar para reunir evidencia. Las sesiones de revisión de evidencia se pueden programar al final de la entrevista.

Página 32

Definición de criterios de evaluación de riesgos

Introducción

Los criterios de evaluación de riesgos son las declaraciones numéricas y en lenguaje sencillo que una organización utiliza para evaluar su riesgo de ciberseguridad. La forma más familiar de cálculos de riesgo, "Riesgo = Probabilidad x Impacto "es la base para el análisis de riesgos en la RAM CIS. Pero es solo el punto de partida para el análisis de riesgos.

Los criterios de evaluación de riesgos deben ser significativos para las organizaciones que los utilizan, por lo que deben ser

vinculado al beneficio y daño potencial que la organización puede crear. El impacto de un
La violación de la seguridad cibernética puede dañar a la organización misma, puede dañar la capacidad de la organización para cumplir con éxito su misión, o puede dañar a otros.

Debido a que las fallas de ciberseguridad pueden dañar a las partes tanto dentro como fuera de una organización, el riesgo Los criterios de evaluación deben ser universalmente significativos y deben abordar los intereses de todos partes potencialmente afectadas. Además, los criterios de evaluación de riesgos deben demostrar a las autoridades que la organización considera el riesgo de daño a otros tanto como el riesgo de daño a ellos mismos, como se indica en el Principio 1.

Si bien estos requisitos pueden parecer complejos, el método presentado en esta sección Abordarlos suficientemente utilizando una técnica que sea fácil de desarrollar y usar.

Criterios de evaluación de riesgos Fundamentos

El análisis de riesgos proporcionado en el CIS RAM es, en su raíz, una cuestión de equilibrio entre el potencial de daños futuros contra la cierta carga de una salvaguardia. Los reguladores y litigantes tienen durante mucho tiempo consideró este equilibrio como clave para actuar como una "persona razonable". La estructura central de un La declaración de riesgo se proporciona a continuación para ilustrar el concepto central de equilibrio.

Figura 3 - Balance dentro del análisis de riesgo central

Observe algunas cosas de inmediato con el modelo de análisis de riesgos en la Figura 3.

- Si bien las organizaciones generalmente evalúan el riesgo observado para determinar si deberían abordarlo o aceptarlo, esta declaración de riesgo compara deliberadamente el riesgo observado con un salvaguarda propuesta.
- El criterio que evalúa el riesgo también evalúa la salvaguarda.
- El impacto del riesgo estima el potencial de daño para la organización y el daño potencial contra otros.

Los evaluadores de riesgos comparan los riesgos con sus salvaguardas propuestas para determinar si las salvaguardas crearían un riesgo previsiblemente menor que el estado actual. Para lograr esto, el el evaluador evalúa el riesgo estatal actual (o "riesgo observado") y la salvaguarda propuesta utilizando Los mismos criterios para garantizar la comparabilidad.

Esta comparación evita que las organizaciones implementen salvaguardas excesivamente pesado, o que crea nuevos riesgos inaceptables. Por ejemplo, una organización que usa software que ya no es compatible con el proveedor, pero depende de ese software para negocios críticos

Page 33

propósitos, deben encontrar métodos alternativos para identificar y controlar posibles riesgos de seguridad hasta que reemplacen el software. Si la gerencia recomienda cambiar rápidamente a inferior, pero software seguro, la organización puede sufrir un mayor impacto en su misión que la seguridad riesgo que están tratando de evitar.

Al considerar CIS Control 18: Seguridad del software de aplicación, se puede hacer una declaración de riesgo para estimar la previsibilidad de una amenaza impactante. El riesgo puede establecerse tal como aparece en la Tabla 9 (donde el puntaje de riesgo '6' es un producto de la probabilidad '2' y el puntaje de impacto más alto '3'):

Tabla 9 - Ejemplo de declaración de riesgo central

Riesgo observado	Impacto de probabilidad de Nosotros	Impactar a Otros	Riesgo Puntuación
Los hackers pueden explotar a los no compatibles, Pero aplicación crítica.	2	2	3	**6 6**

Un evaluador de riesgos debería recomendar y evaluar una salvaguarda para reducir lo inaceptable alto riesgo de seguridad, como se ilustra en la Tabla 10. Aquí, la organización se daría cuenta de que La probabilidad de un impacto negativo en su misión es mayor que el riesgo estatal actual. Esto es un caso obvio de que la carga es mayor que el riesgo, y una salvaguarda recomendada es inaceptable.

Tabla 10 - Ejemplo de salvaguarda propuesta irrazonable

Propuesto Salvaguardia	Nuevo riesgo	Probabilidad	Impactar a Nosotros	Impactar a Otros	Salvaguardia Riesgo
Reemplazar aplicación con inferior, Aplicación segura.	La solicitud será funcionar ineficientemente	3	3	1	**9 9**

Cuando se enfrenta a este análisis, la organización debe encontrar otra forma de abordar el riesgo. Este proceso se describirá más adelante en este capítulo en la sección Tratamiento de riesgos Recomendaciones

Pero lo que debería ser evidente es que sin una definición de los criterios de evaluación de riesgos, la probabilidad y los puntajes de impacto no son significativos. ¿Qué significaría el impacto o la probabilidad de '1', '2' o '3'? ¿de todas formas? La organización necesitará crear definiciones para sus puntuaciones de probabilidad e impacto para que que son significativos para todas las partes interesadas y que proporcionan un método consistente para evaluación de riesgo.

Definiciones de impacto

Las organizaciones de nivel 1 no tienen un alto grado de atención por parte de la gerencia en la operación riesgo de ciberseguridad. En tales organizaciones, los criterios de evaluación de riesgos se pueden desarrollar de manera simple términos que son apropiados para el negocio, pero que no utilizan las justificaciones comerciales que los gerentes a menudo necesitan para tomar decisiones.

Los criterios de evaluación de riesgos se componen de definiciones de impacto y definiciones de probabilidad. En su forma más simple, una definición de impacto debe considerar la misión de la organización (el valor la organización proporciona a otros) y sus obligaciones (el daño que puede causar a otros sin salvaguardas apropiadas). Un modelo de impacto simple para la organización de ejemplo descrita en El Capítulo 1 puede parecerse a la Tabla 11.

Tabla 11 - Definiciones de impacto de ejemplo

Impacto Puntuación	Impacto a nuestra misión	Impacto a nuestras obligaciones
	Misión: proporcionar información para ayudar Los pacientes remotos se mantienen saludables.	*Obligaciones: los pacientes no deben ser perjudicados por información comprometida.*
1	Los pacientes continúan accediendo a útiles información y resultados están en camino.	Ningún daño vendría a los pacientes.
2	Algunos pacientes no pueden acceder al información que necesitan para obtener buenos resultados.	Pocos pacientes pueden sufrir daños después de compromiso de información o servicios.
3	Ya no podemos proporcionar ayuda información a pacientes remotos.	Muchos pacientes pueden sufrir daños financieros, reputacional o físicamente, hasta y incluyendo la muerte

Tenga en cuenta que esta organización de ejemplo, un fabricante de tecnología de salud y proveedor de servicios, tiene definió el impacto a su servicio como su "misión" y el impacto a los demás como su "obligación". Están definiendo su misión en términos de su valor para su circunscripción (pacientes que usan su servicio) y sus obligaciones para evitar daños a esos pacientes debido a una violación de la información.

Antecedentes: definiciones de impacto

Este documento proporciona instrucciones para definir los impactos y los puntajes de impacto (magnitudes) en esta sección con instrucciones más detalladas y ejemplos en las "Técnicas de análisis de riesgos"

capítulo. El lector debe comprender antes de continuar que las organizaciones en la mayoría de los casos no debe definir impactos exclusivamente utilizando valores financieros. Si bien el costo es común y consideración casi necesaria al evaluar riesgos y salvaguardas, si es el único criterio, la organización se comunicará con su personal, así como con las partes interesadas y autoridades, ese costo es su única preocupación. El propósito que sirve la organización y el el daño que pueda ocurrir a otros debe ser parte de la evaluación si el riesgo se debe vincular responsablemente con el potencial de daño, y si la evaluación debe ser comprensible para los reguladores y legales autoridades.

Las organizaciones también deberían considerar tener más de tres tipos de impacto en su impacto definiciones si tienen más de una misión, múltiples objetivos y muchas obligaciones que deben tener en cuenta en su análisis de riesgos. Si bien esta expansión puede crear una creciente amplio registro de riesgos, puede ayudar a las organizaciones a sentirse cómodas todos los intereses relevantes fueron considerado en su análisis de riesgos.

También tenga en cuenta que el puntaje de impacto de '1' (que está sombreado en gris para separarlo de los puntajes más altos) describe los impactos que generalmente se entenderían aceptables. Si una violación condujo a una situación donde los pacientes continuaron accediendo a información útil, y no hubo daños previsibles para pacientes, entonces, por supuesto, eso se interpretaría como un impacto aceptable. La organización no debe estar satisfecho con una violación que no tuvo impacto (sus procedimientos de respuesta a incidentes deberían identificar una causa raíz y abordarla para que la violación no vuelva a ocurrir), pero en términos de riesgo planificación, dicho riesgo podría considerarse "aceptable".

El puntaje de impacto de '2' se usaría para estimar un riesgo en el cual el daño llegaría a la misión de ayudar a pacientes remotos, o si algún daño puede llegar a los pacientes que confían en el confidencialidad, integridad y disponibilidad de información. Un impacto a un nivel de '2' sería considerado 'no aceptable' por la organización, sus clientes, agencias reguladoras o litigantes.

Página 35

Por lo tanto, los riesgos previsibles (una probabilidad de '2') que se estiman con un impacto de '2' probablemente no serían considerado "aceptable", pero un riesgo imprevisible (puntaje de probabilidad de '1') que crearía un el impacto de '2' sería aceptable ya que el impacto se considera no previsible.

El puntaje de impacto de '3' podría considerarse 'catastrófico' o 'alto'. La misión fallaría completamente, y las obligaciones con los clientes pacientes podrían dañar a muchas personas, hasta e incluyendo muerte (presumiblemente porque la información de salud era inexacta o no estaba disponible cuando era críticamente necesario).

Con estos criterios de impacto definidos de esta manera, el proveedor de información de salud podría estimar impacto parte del riesgo de manera consistente. Cierta cantidad de conocimiento sobre cómo los riesgos crearían esos impactos serían necesarios mientras se realiza la evaluación de riesgos, pero bien informados los gerentes y el personal podrían proporcionar estimaciones plausibles de riesgo de manera consistente utilizando Estas definiciones de impacto.

Se proporciona una explicación detallada de cómo desarrollar definiciones de impacto con múltiples ejemplos en el capítulo "Técnicas de análisis de riesgos".

Definiciones de probabilidad

Este método de evaluación de riesgos describe la probabilidad en términos de previsibilidad. Mientras que la probabilidad de riesgo A menudo se describe en términos de probabilidad estadística, CIS RAM favorece la previsibilidad porque utiliza terminología simple que se alinea con la práctica comercial común, así como con los requisitos legales y reglamentarios lenguaje utilizado para determinar la razonabilidad de las salvaguardas que reducen los riesgos. Recomendaciones para alinear este modelo de probabilidad con los métodos de probabilidad se proporcionan en el "Análisis de riesgo Capítulo de Técnicas. Al combinar la probabilidad con la previsibilidad, las organizaciones pueden beneficiarse de tanto análisis basado en datos como análisis de debida atención.

La definición de probabilidad para una organización de Nivel 1 podría ser simplemente construida, similar en estructura y profundidad de las definiciones de impacto como se muestra en la Tabla 12.

Tabla 12 - Ejemplos de definiciones de probabilidad

Probabilidad Puntuación	Previsibilidad
1	**No es previsible** . Esto no es plausible en el medio ambiente.

2	**Previsible** . Esto es plausible, pero no esperado.
3	**Esperado.** Estamos seguros de que esto ocurrirá en algún momento.

- "No previsible" implica que una amenaza no es plausible en el entorno que se está juzgado. La pérdida de medios portátiles puede no ser previsible durante una evaluación de riesgos de un aplicación alojada
- "Previsible" implica algo plausible, pero la organización sería sorprendido si ocurrió. Un ejecutivo fundador que lleva copias de datos confidenciales a los competidores pueden considerarse previsibles, incluso si no se espera.
- "Esperado" implica una amenaza que no es común, pero que eventualmente sucedería. Se pueden esperar ataques de phishing u otros ataques de ingeniería social en muchos ambientes.

Cuando los evaluadores de riesgos estiman la probabilidad de una amenaza, seleccionarán los puntajes '1', 2 'o' 3 'usando la definición de previsibilidad como su guía. Las organizaciones pueden agregar límites basados en el tiempo a sus definiciones de previsibilidad (es decir, "previsible dentro de los umbrales de planificación", "esperado dentro de los cinco plan anual "o" No previsible en el próximo año fiscal "). Si las organizaciones introducen límites de tiempo para sus definiciones de probabilidad deben priorizar las inversiones en tratamiento de riesgos para cumplir con estos

Page 36

cronogramas Eso puede ser un desafío excesivo para muchas organizaciones, por lo que deben proceder con cuidado.

La simplicidad de estas definiciones ayudará a las organizaciones de Nivel 1 a obtener de manera rápida y consistente estimar si esperan que ocurran riesgos impactantes.

Ejercicio :

El lector debe desarrollar los criterios de evaluación de riesgos de su organización utilizando los "Criterios: Hoja de trabajo de Nivel 1 "que se proporciona en el documento complementario *CIS_RAM_Workbook.*

El lector debe considerar:

1. Trabajar con un patrocinador de gestión empresarial que pueda ayudar a garantizar que la Misión y las definiciones de obligaciones son sensibles para la organización.
2. Trabajar con un asesor legal para ayudar a garantizar que las definiciones de impacto aborden los intereses. de todas las partes potencialmente afectadas, y para asegurar que aparezcan declaraciones de impacto equitativo para todas las partes.
3. Consulte la guía para definir y calificar los tipos de impacto en el "Análisis de riesgos Capítulo de Técnicas.

El evaluador de riesgos necesitará usar su juicio profesional para definir los tipos de impacto y describir los niveles de impacto que la organización debe lograr. Porque los criterios de evaluación de riesgos son una declaración de la organización de lo que lograrán en términos de daño a sí mismos y dañar a otros, las organizaciones deben consultar con un asesor legal antes de finalizar estos criterios y tomar decisiones de riesgo basadas en ellos.

Definición de criterios de aceptación de riesgos

Introducción

Debido a que las evaluaciones de riesgo son esencialmente cuestiones de equilibrio, los criterios para aceptar el riesgo debería ayudar a determinar si se logró el equilibrio. En CIS la aceptación del riesgo RAM tiene dos componentes:

- Riesgo apropiado: que la probabilidad de un impacto debe ser aceptable para todos previsiblemente partes afectadas
- Riesgo razonable: que el riesgo planteado por una salvaguarda debe ser menor o igual al riesgo contra el que protege.

Si bien estos componentes se han demostrado brevemente en el Capítulo 1, el "riesgo apropiado"

se describirá con más detalle en esta sección. El "riesgo razonable" se describirá más adelante en el Riesgo Sección de recomendaciones de tratamiento más adelante.

Recuerde que las definiciones de impacto fueron redactadas de modo que las definiciones de impacto aceptables parecieran apropiado para cualquier persona que los lea. Para organizaciones de nivel 1 que usan una puntuación de impacto rango de '1' a '3' el rango de puntajes de impacto aceptables es simplemente '1'. Definiciones de impactos eso obtendría al menos un '2', por lo tanto, representaría los impactos que una organización, y presumiblemente sus partes interesadas, encontrarían inaceptable.

Tabla 13 - Impactos inaceptables

Impacto Puntuación	Impacto a nuestra misión	Impacto a nuestras obligaciones
	Misión: proporcionar información para ayudar Los pacientes remotos se mantienen saludables.	*Obligaciones: los pacientes no deben ser perjudicados por información comprometida.*
1	Los pacientes continúan accediendo a útiles La información y los resultados están en camino.	Ningún daño vendría a los pacientes.
2	Algunos pacientes no pueden acceder al información que necesitan para obtener buenos resultados.	Pocos pacientes pueden sufrir daños después de compromiso de información o servicios.
3	Ya no podemos proporcionar ayuda información a pacientes remotos.	Muchos pacientes pueden sufrir daños financieros, reputacional o físicamente, hasta y incluyendo la muerte

Del mismo modo, los puntajes de probabilidad para las organizaciones de Nivel 1 oscilaron entre '1' y '3', donde el puntaje de '2' representó el puntaje más bajo de "previsibilidad".

Tabla 14 - Probabilidad inaceptable

Probabilidad Puntuación	Previsibilidad
1	**No es previsible** . Esto no es plausible en el medio ambiente.
2	**Previsible** . Esto es plausible, pero no esperado.
3	**Esperado.** Estamos seguros de que esto ocurrirá en algún momento.

Las organizaciones de nivel 1 deberían determinar que protegerían contra los riesgos que alcanzaron un umbral de inaceptabilidad; por ejemplo, riesgos que podrían *prever previsiblemente* (la probabilidad es '2') *prevenir pacientes de tener acceso a la información* (el impacto es '2') o *causar una violación que puede dañar pacientes* (el impacto es '2'). Entonces, si Riesgo = Impacto x Probabilidad, entonces la organización invertiría contra riesgos que se puntúan '4' o más. *¡Todos los riesgos más bajos pueden ser aceptados!*

Tabla 15 - Criterios de aceptación del riesgo

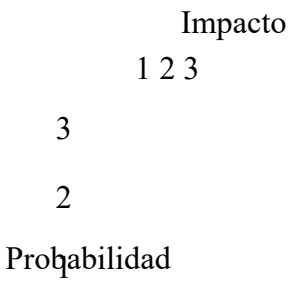
Impacto Límite	X	Probabilidad Límite	=	Riesgo Límite
2	X	2	=	4 4
		… por lo tanto …		
Riesgo aceptable			<	**4 4**

Considere cómo se describiría *un* riesgo *razonable* : si un riesgo *no puede predecirse* (la probabilidad es '1') evitar que la organización *brinde información útil a los pacientes* (el impacto es '3'), entonces *eso es aceptable.* Suena aceptable para personas razonables, y 1 x 3 = 3, que es menor que 4.

Vea también cómo funciona el cálculo cuando se produce un impacto aceptable de *no dañar a los pacientes* ('1') *se espera que ocurra* ('3'). 1 x 3 = 3, que nuevamente es menor que '4'. Este es un riesgo aceptable. Mientras los mapas de calor de riesgo no se usan en CIS RAM, las organizaciones ahora pueden considerar que los mapas de calor pueden

representar la aceptabilidad real del riesgo según los requisitos de la organización y un deber de cuidado para otros.

Figura 4 - Ejemplo de mapa de calor de riesgo



Ejercicio :

El lector debe definir los criterios de aceptación de riesgos de su organización utilizando los "Criterios - Nivel Hoja de trabajo de 1 "que se proporciona en el documento complementario *CIS_RAM_Workbook* .

El lector debe considerar:

1. Trabajar con un patrocinador de gestión empresarial que pueda ayudar a garantizar que el riesgo Los criterios de aceptación son sensibles para la organización.
2. Trabajar con un asesor legal para ayudar a garantizar que la definición de aceptación del riesgo aborda los intereses de todas las partes potencialmente afectadas y para garantizar ese impacto Las declaraciones parecen equitativas para todas las partes.

El evaluador de riesgos necesitará usar su juicio profesional para identificar niveles de riesgo aceptables. Debido a que los criterios de aceptación del riesgo son una declaración de la organización de lo que tolerarán en términos de daño a sí mismos y daño a otros, las organizaciones deben consultar con un asesor legal antes de finalizar estos criterios y tomar decisiones de riesgo basadas en ellos.

Un proceso de evaluación de riesgos basado en el control

Introducción

Organizaciones de nivel 1 que usan los controles CIS, pero que no han establecido una capacidad sólida para gestionar el riesgo de ciberseguridad, las evaluaciones de riesgo basadas en el control son adecuadas para sus necesidades.

Este método de evaluación de riesgos CIS está diseñado para ayudar a las organizaciones a utilizar el CIS de manera responsable Controles en la medida en que son capaces, incluso si los controles no se pueden implementar por completo. El método de evaluación de riesgos ayuda a las organizaciones de nivel 1 a:

1. Modelar salvaguardas basadas en los Controles CIS V7 que aborden sus riesgos, mientras trabajan dentro de sus limitaciones.
2. Priorizar las salvaguardas que deben implementar, en función de los riesgos de su organización.

Página 39

3. Desarrollar un plan práctico para implementar los Controles CIS V7 a lo largo del tiempo y como recursos permiso.
4. Documente por qué su método para aplicar CIS Controls V7 es razonable, dado el equilibrio entre su riesgo y sus recursos.

Esta sección describirá un registro de riesgos que está disponible como plantilla en el documento complementario documento *CIS_RAM_Workbook* .

El registro de riesgos

Hasta este punto, la organización ha identificado los activos de información o las clases de activos que Se evaluará el riesgo. También han desarrollado criterios de evaluación de riesgos y aceptación de riesgos. criterios Usando la plantilla de registro de riesgos provista en el documento complementario *CIS_RAM_Workbook* , la organización verá una lista de controles y subcontroles CIS que actuarán como el índice principal, o conductor, para modelar sus riesgos.

En la Figura 5 se muestra un mapa de diseño del registro de riesgos para una organización de Nivel 1.

Figura 5 - Mapa de diseño del registro de riesgos

El registro de riesgos para organizaciones de Nivel 1 es una lista de riesgos identificados y su riesgo recomendado tratamientos, también conocidos como "salvaguardas". Cada fila representa un riesgo y un tratamiento de riesgo recomendación. Las partes del registro de riesgos son:

A. Los encabezados de columna y el texto guía ayudan al lector o al evaluador de riesgos a comprender el información contenida en la columna.
B. Los controles CIS ayudan al evaluador de riesgos a considerar los controles que deberían estar en su lugar para Proteger los activos de información.
C. Se identifican los activos de información dentro del alcance o las clases de activos.
D. El "modelo de amenaza" incluye los siguientes tres elementos:
    a. Cómo implementa la organización el Control CIS (si lo hacen) para proteger el activo de información o clase de activo.
    si. La vulnerabilidad que puede existir si el control no se implementa completamente.

Page 40

do. La amenaza que puede comprometer el activo debido a la vulnerabilidad.

E. La evaluación de riesgos estima la probabilidad de que la amenaza tenga éxito y la impactos a la misión y obligaciones si lo hiciera. Luego se calcula el puntaje de riesgo resultante como producto de la probabilidad y la mayor de las dos puntuaciones de impacto.

F. Los tratamientos de riesgo se recomiendan para los riesgos que se evalúan como inaceptablemente altos. Se describen las salvaguardas que se basan en los Controles CIS V7, y a su vez son evaluado por el riesgo que pueden representar para la misión y los objetivos. Un "riesgo de salvaguardia" Se calcula la puntuación que debe ser inferior a los criterios de aceptación del riesgo, y el riesgo que se pretende abordar

El proceso

El evaluador de riesgos analizará cada riesgo siguiendo los siguientes pasos como se muestra en el diagrama de la Figura 6.

Figura 6 - Diagrama de análisis de riesgos de nivel 1

1. Uso de la plantilla de registro de riesgos para organizaciones de Nivel 1 que se proporciona en *CIS_RAM_Workbook* , lea y considere el Control CIS que se indica en uno de los riesgos registrar filas
2. Seleccione los activos de información o las clases de activos que se enumeran en el inventario de activos. Grabar los activos seleccionados en la celda "Activo de información" en esa fila.
    a. Si hay múltiples activos de información o clases de activos a considerar para cada CIS Control, enumere todos en una celda en la columna de activos de información o agregue Múltiples filas para el Control CIS para que se analice cada activo de información por separado. *La decisión debe basarse en cuán granular es el evaluador de riesgos. preparado para estar en su análisis y planificación, y qué tan útil es la distinción entre activos sería* .
3. Reúna evidencia de qué tan bien se aplica el Control CIS contra la información seleccionada bienes.
    a. La evidencia puede ser en forma de entrevistas, una revisión de configuraciones o una revisión de evidencia, como registros y registros. Este paso requiere conocimiento y experiencia en la detección de vulnerabilidades y la comprensión de las amenazas de seguridad. Los métodos para reunir evidencia se proporcionan en el capítulo "Análisis de riesgos Técnicas.
4. Describa la salvaguarda que implementa los controles CIS y cómo es la salvaguarda aplicado en la organización en la celda "Control actual" de esa fila.
5. Considere la diferencia entre el Control CIS y la salvaguarda actualmente utilizada y determinar si existe una deficiencia en cómo se implementa actualmente el control y operando. Si el control actual no se implementa como se describe, ¿cómo sería esto? descrito como una vulnerabilidad?

Page 41

a. Considere el objetivo del control CIS. Por ejemplo, CIS Control 2.3 estados "Utilice herramientas de inventario de software en toda la organización para automatizar documentación de todo el software en los sistemas empresariales ". El objetivo del subcontrol es detallar todos los sistemas operativos y aplicaciones que están en uso para que La organización sabe qué software debe controlar. Si el control actual no cumplir el objetivo, luego declarar la brecha como una vulnerabilidad en la celda de vulnerabilidad, tales como: "No tenemos una lista actual actualizada automáticamente

sistemas operativos o aplicaciones que operan en nuestros sistemas ".

6. Ahora considere la amenaza que podría ocurrir debido a la vulnerabilidad.
    a. La vulnerabilidad anterior podría combinarse con la amenaza: "Malware o piratas informáticos podría aprovechar las vulnerabilidades de software que no conocíamos o proteger contra."
7. Luego, calcule la probabilidad de que la amenaza tenga éxito y el impacto que puede crear.
    a. La estimación de probabilidad puede ser un desafío al principio, pero los criterios de evaluación de riesgos fue desarrollado para proporcionar alguna orientación en ese proceso de estimación. Promover Se proporciona orientación en el capítulo "Técnicas de análisis de riesgos" más adelante en este documento.
    si. Los puntajes de impacto deben proporcionar estimaciones del impacto que tal amenaza causaría crear. Considere las puntuaciones de probabilidad e impacto como un par. En otras palabras, "¿Cuál es la probabilidad de que resulte este impacto?" Proporcionar más orientación.
8. La puntuación de riesgo se calculará automáticamente multiplicando la puntuación de probabilidad por mayor de los dos puntajes de impacto.

Nivel 1 Evaluación de riesgos Ejemplo 1: saber si una salvaguardia actual es suficiente

Examinemos cómo funciona este proceso utilizando análisis de riesgos para nuestra organización de Nivel 1 de ejemplo.

Mientras realiza su evaluación de riesgos, la organización comienza con CIS Control 1.1 que les indica que implementen una herramienta automatizada de descubrimiento de inventario de activos. Ellos saben que no tienen dicha herramienta, y les preocupa el tiempo y el costo potencial de investigar y obtener uno. Además, no saben si esta debería ser su máxima prioridad, dados otros elementos que están en su mente, como el fortalecimiento de los dispositivos de campo y la gestión de vulnerabilidades. Mientras CIS Controles V7 proporciona una guía clara sobre la importancia de este importante control, puede haber otros áreas de preocupación que deben abordarse antes, en función del entorno de la organización.

Usando la plantilla de registro de riesgos para organizaciones de Nivel 1, la organización de ejemplo primero revisa El control que están analizando.

Tabla 16 - Ejemplo de control CIS Control CIS 1.1

CEI Controlar	Descripción
1.1	Utilice una herramienta de descubrimiento activa para identificar dispositivos conectados a red de la organización y actualizar el inventario de activos de hardware.

El evaluador de riesgos considera el activo de información que protegería el control. En este caso, ellos aplicaría una herramienta de descubrimiento de inventario de activos a todos los dispositivos conectables a la red. Podrían enfocarse puramente en una clase de activos, como estaciones de trabajo portátiles, "sin cabeza" o "internet de las cosas" dispositivos, teléfonos inteligentes, computadoras portátiles o dispositivos en una red específica, como la VLAN corporativa que se usa para conectar dispositivos inalámbricos. Pero para simplificar las cosas para su primera evaluación, ellos decida que la clase de activo que evaluarán será "todos los dispositivos".

Tabla 17 - Ejemplo de activo de información de nivel 1

Activo de información
Todos los dispositivos.

Luego, deben pensar y registrar cuál es su control actual, qué resulta pueden existir vulnerabilidades y qué amenazas les preocuparán. Se dan cuenta de que no tienen una herramienta automatizada que proporcione un inventario regular, pero tienen una vulnerabilidad herramienta de escaneo que utilizan ocasionalmente. Eso puede ser útil aquí.

Pero el control claramente tiene un objetivo, que es la detección automática de todos los sistemas que aparecer en la red. Si la organización ocasionalmente usa un escáner de vulnerabilidades, entonces un La vulnerabilidad relacionada con este control sería que los nuevos sistemas podrían unirse a la red y no ser detectado hasta que se produjo el siguiente análisis de vulnerabilidad. La amenaza resultante sería obvia: Los sistemas comprometidos pueden operar en la red entre escaneos.

Entonces las siguientes tres columnas se verían así:

Tabla 18 - Ejemplo de modelo de amenaza

Controlar	Vulnerabilidad	Amenaza
Escaneos de vulnerabilidad ocurrir ocasionalmente y puede no identificar a todos sistemas que tienen estado en la red entre escaneos.	Sistemas que se han unido al red entre escaneos esporádicos No será detectado.	Hackers o malware pueden ataque y control sistemas que no tienen ha sido detectado, controlado, y monitoreado

Ahora que la amenaza ha sido modelada, el evaluador de riesgos debe estimar la probabilidad y impacto del riesgo. La organización debe considerar la probabilidad de que ocurra un impacto si el La amenaza tuvo éxito. Los evaluadores de riesgos deben pensar en la probabilidad y el impacto como dependiente emparejamiento. En este ejemplo, la organización puede creer que múltiples sistemas se unirán y se irán su red sin detección. Ese es un escenario muy probable para ellos. Pero también pueden cree que el riesgo es previsible pero inesperado para que un sistema no detectado cause un impacto si Los visitantes que reciben son empleados de organizaciones asociadas bien aseguradas.

En términos del impacto que las personas pueden sufrir, el evaluador de riesgos considera cómo podría ser el daño hecho en este escenario previsible pero poco probable. Si un empleado de un socio seguro traería en una computadora portátil que estaba infectada con malware que podría propagarse a otros sistemas de la red, ¿Qué daño podría hacer eso? Si estos empleados asociados se unen a una red que contiene una mezcla de sistemas, algunos con información altamente sensible, entonces es previsible pero no se espera que el escenario podría exponer registros que podrían causar daño a pocos pacientes, o muchos pacientes? haría la misión se reduzca al punto de que algunos pacientes no puedan obtener información que pueda mejorar los resultados de salud?

La organización determina que es previsible pero no esperado que los registros de muchos pacientes pueden estar expuestos en el escenario de riesgo que modelaron. No creen que el escenario de riesgo afectaría su misión. Así que ahora agregarán esta información a su registro de riesgos para ver cómo El riesgo se evalúa.

Recuerde las definiciones de los puntajes de impacto y probabilidad que creó la organización. Impacto los puntajes se definieron anteriormente como se muestra en la Tabla 19.

Page 43

Tabla 19 - Definiciones de impacto de ejemplo

Impacto Puntuación	Impacto a nuestra misión	Impacto a nuestras obligaciones
	Misión: proporcionar información para ayudar Los pacientes remotos se mantienen saludables.	*Obligaciones: los pacientes no deben ser perjudicados por información comprometida.*
1	Los pacientes continúan accediendo a útiles información y resultados están en camino.	Ningún daño vendría a los pacientes.
2	Algunos pacientes no pueden acceder al información que necesitan para obtener buenos resultados.	Pocos pacientes pueden sufrir daños después de compromiso de información o servicios.
3	Ya no podemos proporcionar ayuda información a pacientes remotos.	Muchos pacientes pueden sufrir daños financieros, reputacional o físicamente, hasta y incluyendo la muerte

La puntuación de impacto '1' está sombreada para indicar que se considera un impacto aceptable para todas las partes. también recuerde que la probabilidad se definió con la siguiente tabla.

Tabla 20 - Definiciones de probabilidad de ejemplo

Probabilidad Puntuación	Previsibilidad
1	**No es previsible** . Esto no es plausible en el medio ambiente.

2	**Previsible** . Esto es plausible, pero no esperado.
3	**Esperado.** Estamos seguros de que esto ocurrirá.

Un riesgo que es previsible pero que no se espera que ocurra (probabilidad = 2) de una manera que no crea impacto en la misión (impacto de la misión = 1), pero eso crearía daño a muchos pacientes (impacto de las obligaciones = 3) aparecería de la siguiente manera.

Tabla 21 - Ejemplo de estimación de riesgo

Amenaza Probabilidad	Misión Impacto	Obligaciones Impacto	Puntuación de riesgo
2	1	3	6 6

El puntaje de riesgo es el producto del puntaje de probabilidad y el más alto de los dos puntajes de impacto, que en este caso es '2 x 3 = 6'.

Recuerde también que los criterios de aceptación de riesgos para la organización de Nivel 1 se veían así:

Tabla 22 - Criterios de aceptación del riesgo

Impacto Límite	X	Probabilidad Límite	=	Riesgo Límite
2	X	2	=	4 4
		… por lo tanto …		
Riesgo aceptable			<	4 4

Page 44

Porque el riesgo aceptable es cualquier cosa por debajo de '4', y el riesgo observado asociado con el Control CIS 1.1 es '6', el riesgo es inaceptablemente alto.

Podemos unir estos elementos para ilustrar el punto más claramente. (Mientras el registro de riesgos en el libro de trabajo muestra este ejemplo en formato horizontal, este riesgo se muestra en formato vertical para facilitar la lectura en este documento).

Tabla 23 - Ejemplo de riesgo para el control CIS 1.1

Análisis de riesgo	Valor
Control CIS	1.1
Descripción	Utilice una herramienta de descubrimiento activa para identificar dispositivos conectados a red de la organización y actualizar el inventario de activos de hardware.
Activo de información	Todos los dispositivos.
Controlar	Los escaneos de vulnerabilidad ocurren ocasionalmente y pueden no identificar todos sistemas que han estado en la red entre escaneos.
Vulnerabilidad	Los sistemas que se han unido a la red entre escaneos esporádicos No ser detectado.
Amenaza	Los hackers o malware pueden atacar y controlar sistemas que no sido detectado, controlado y monitoreado.
Probabilidad de amenaza	2
Impacto de la misión	1
Obligaciones Impacto	3
Puntuación de riesgo	**6 6**
Aceptabilidad del riesgo	**Inaceptable**

Entonces, la organización se da cuenta, en base a sus propios criterios para calificar y aceptar el riesgo, que su el uso ocasional de escaneos de vulnerabilidad no es suficiente para abordar el riesgo de sistemas infectados unirse a la red. Este riesgo no es aceptable porque no es "apropiado" (su riesgo es mayor que la puntuación aceptable de "menos de 4.")

Pero no están seguros de qué hacer con este riesgo, porque no saben si serán capaz de permitirse el tiempo o el presupuesto para implementar una solución más robusta para CIS Control 1.1 (como un dispositivo de control de acceso a la red) y tienen muchos más controles y riesgos a considerar. El método para identificar formas razonables de implementar salvaguardas se abordará en el Recomendaciones de tratamiento de riesgos más adelante en este capítulo.

Primero, sin embargo, examinaremos algunos controles más de CIS y veremos cómo funciona el Nivel 1 La organización los analiza.

Nivel 1 Evaluación de riesgos Ejemplo 2 - Aceptabilidad del riesgo en diferentes contextos

Más adelante en la evaluación de riesgos, la organización de Nivel 1 considera que CIS Control 3.4 dice: "Implemente herramientas de actualización de software automatizadas para garantizar que los sistemas operativos están ejecutando las actualizaciones de seguridad más recientes proporcionadas por el proveedor de software ". Esta es una control desafiante para muchas organizaciones. Si bien el objetivo de la reparación automática de los sistemas vulnerables son importantes, muchos sistemas y aplicaciones fallarán cuando algo de seguridad Los parches interfieren con su funcionalidad.

Página 45

Por ejemplo, las aplicaciones que dependen de bibliotecas de códigos que se reemplazan con versiones más seguras durante el parcheado puede fallar. Como resultado, muchas organizaciones prueban parches antes de lanzarlos a sistemas activos y aplicaciones.

La organización de Nivel 1 cree que les está yendo bien en este sentido. Tienen dos ambientes; un entorno de producción en el que sus aplicaciones operan en Internet, y un entorno corporativo en el que ejecutan su negocio y desarrollo de aplicaciones medio ambiente. Cuando ejecutan sus escaneos de vulnerabilidad esporádicos en su entorno de producción, responden de inmediato a las vulnerabilidades identificadas que se pueden reparar. De hecho, corren su escaneos de vulnerabilidad cuando reciben información de vulnerabilidades de alto riesgo de una información de amenaza servicio al que se suscriben (para este ejemplo, un proveedor de servicios ficticio llamado "Información de amenazas Servicio"). Su pila de aplicaciones es simple y se basa completamente en implementaciones estándar de El marco de aplicación de los proveedores. Entonces, cuando el proveedor envía parches, se pueden aplicar rápidamente, incluso de forma manual, con poco riesgo para las aplicaciones.

Creen que su riesgo es bajo aquí en términos de seguridad. Pero están preocupados por su paciente. clientes que no pueden usar sus sistemas durante los tiempos de inactividad de parches. Entonces evalúan el riesgo de esta manera.

Tabla 24 - Ejemplo de análisis de riesgos para el control CIS 3.4

Análisis de riesgo	Valor
Control CIS	3.4
Descripción	Implemente herramientas de actualización de software automatizadas para garantizar que los sistemas operativos ejecutan las actualizaciones de seguridad más recientes proporcionado por el proveedor del software.
Activo de información	Todos los dispositivos en el entorno de producción.
Controlar	Los análisis de vulnerabilidad se producen cuando el Servicio de información sobre amenazas anuncia un vulnerabilidad de moderada a alta que necesita revisión. Equipo confiable parchea los sistemas dentro de las 24 horas posteriores al anuncio.
Vulnerabilidad	Una ventana de vulnerabilidad de 24 horas permanece con el proceso actual.
Amenaza	Los hackers o malware pueden atacar y controlar sistemas que no sido reparado dentro del período de 24 horas después de que la vulnerabilidad fue Anunciado.
Probabilidad de amenaza	1
Impacto de la misión	2

Obligaciones Impacto	1
Puntuación de riesgo	**2**
Aceptabilidad del riesgo	**Aceptable**

La organización de Nivel 1 ha determinado que su riesgo está asociado con el Control CIS 3.4, al menos en su entorno de producción, es aceptable porque el riesgo es "apropiado" (su puntaje es menor a '4'). Esto permite a la organización mantener sus procesos actuales en su lugar y enfocarse en riesgos más altos. primero.

Pero todavía tienen una red interna a considerar. En esta red tienen un importante aplicación de gestión empresarial que se basa en un sistema operativo anterior y que no trabajar con parches más avanzados para el sistema operativo. El proveedor de la aplicación dice que lo harán lanzará una versión más segura el próximo año, y la organización de Nivel 1 sabe que la conversión

Página 46

para la nueva versión será muy gravoso. Mientras tanto, tienen sistema operativo vulnerabilidades en el entorno de aplicaciones de gestión empresarial que deben abordarse. Pero tienen miedo de aplicar esos parches porque pueden romper la aplicación.

Evalúan el riesgo en su registro de riesgos con los valores que se enumeran a continuación.

Tabla 25 - Ejemplo de riesgo para el control CIS 3.4

Análisis de riesgo	Valor
Control CIS	3.4
Descripción	Implemente herramientas de actualización de software automatizadas para garantizar que los sistemas operativos ejecutan las actualizaciones de seguridad más recientes proporcionado por el proveedor del software.
Activo de información	Aplicación de gestión empresarial en el corporativo interno red.
Controlar	Los análisis de vulnerabilidad se producen cuando el Servicio de información sobre amenazas anuncia un vulnerabilidad de moderada a alta que necesita revisión. Parches del equipo la mayoría de los sistemas dentro de las 24 horas posteriores al anuncio.
Vulnerabilidad	Los sistemas de aplicaciones de gestión empresarial no tienen parches para más de un año.
Amenaza	Los piratas informáticos o el malware pueden atacar y controlar la empresa entorno de aplicación de gestión.
Probabilidad de amenaza	2
Impacto de la misión	2
Obligaciones Impacto	3
Puntuación de riesgo	**6 6**
Aceptabilidad del riesgo	**Inaceptable**

Claramente tienen un riesgo inaceptable con la forma en que este control protege su red corporativa (el la puntuación de riesgo de '6' es inapropiadamente alta). La aplicación de gestión empresarial está creando un riesgo. eso debería abordarse de alguna manera. La organización abordará este riesgo en los siguientes sección, Recomendaciones de tratamiento de riesgos.

Nivel 1: Evaluación de riesgos Ejemplo 3 - Riesgos priorizados
A medida que la organización de Nivel 1 más tarde considere su riesgo relacionado con el Control CIS 14.9, abordarán un preocupación común sobre la gestión de registros; qué eventos se capturan en registros y repositorios ¿debería centrarse la organización? El Control CIS 14.9 establece: “Aplicar registros de auditoría detallados para acceso a datos confidenciales o cambios a datos confidenciales ".

La organización de nivel 1 sospecha que necesitarán invertir en su gestión de registros y SIEM

tecnologías pronto, pero también son conscientes de que elegir qué mensajes de registro capturar, priorizar y alertar requerirá una cuidadosa reflexión y mucha experiencia. Su principal preocupación con respecto a la gestión de registros está detectando el abuso de los sistemas y el acceso a los datos. La moral ha sido baja, y están en un negocio competitivo que puede hacer que los empleados internos roben datos confidenciales desde su aplicación de gestión empresarial y proporcionarla a un competidor.

Page 47

Están seguros de que no lo están haciendo lo suficientemente bien con su revisión del registro de acceso ahora, pero lo harán analizar este riesgo para evaluar y priorizar este riesgo. También utilizarán su análisis de tratamiento de riesgos. más adelante para determinar qué configuraciones de administración de registros son apropiadas para su empresa Aplicación de gestión.

Tabla 26 - Ejemplo de riesgo para el control CIS 14.9

Análisis de riesgo	Valor
Control CIS	14,9
Descripción	Aplicar registros de auditoría detallados para acceder a datos confidenciales o cambios a datos confidenciales.
Activo de información	Aplicación de gestión empresarial
Controlar	Los registros de acceso se capturan y almacenan localmente, y no se revisan.
Vulnerabilidad	La organización desconoce el uso sospechoso o inapropiado.
Amenaza	Los empleados o hackers no autorizados pueden usar privilegios escalados y puede acceder y abusar de información no pública en la aplicación.
Probabilidad de amenaza	3
Impacto de la misión	2
Obligaciones Impacto	3
Puntuación de riesgo	**9 9**
Aceptabilidad del riesgo	**Inaceptable**

Después de haber ingresado algunos riesgos en el registro de riesgos, este análisis no los sorprende. Ellos estaban seguros de que al revisar este control destacarían un problema. Y ahora ven que este riesgo es inapropiadamente alto y debe priorizarse sobre los otros riesgos que analizado previamente Para cuando se complete la evaluación de riesgos, este riesgo se ubicará entre los primeros elementos que deben abordarse (tiene el puntaje de riesgo máximo de '9'). Ellos seleccionarán y diseñe su salvaguarda de tratamiento de riesgo en el siguiente paso, Recomendaciones de tratamiento de riesgo.

48

Ejercicio :

El lector debe consultar la plantilla Registro de riesgos - Nivel 1 que se proporciona en el documento complementario *CIS_RAM_Workbook* . Pueden usar la plantilla de registro de riesgos para ingrese un conjunto de riesgos asociados con los Controles CIS y los activos de información que están en Alcance de su evaluación.

Al hacer este ejercicio, el lector debe considerar:

1. Cuando un control CIS puede establecerse adecuadamente para todo el alcance, un activo clase o un activo de información independiente.
2. Establecer al menos un riesgo por control CIS. Un control CIS puede aparecer varias veces si Las clases de activos y los activos de información utilizan el control de manera diferente.
3. Si un control o activo de información requiere un examen para comprender su valor real configuración y efectividad.
4. Si la organización puede tolerar la cantidad de esfuerzo y tiempo que el riesgo evaluación requiere.
    a. Las organizaciones no deberían tratar de "hervir el océano". Una evaluación de riesgos solo puede completarse utilizando los recursos disponibles.
    si. La organización debe usar análisis de alto nivel (revisión de políticas y entrevistas) si no tienen mucho tiempo y recursos.
    do. Los activos de información deben ser probados y examinados con más detalle a medida que pasa el tiempo. permite.
    re. La organización debe planificar evaluaciones de riesgos recurrentes para identificar más riesgos. a través del tiempo.
5. Colaborar con expertos en temas de seguridad de la información para ayudar a modelar amenazas que son previsibles en el medio ambiente, y para ayudar a evaluar la efectividad de salvaguardas actuales.

El evaluador de riesgos deberá usar su criterio profesional para seleccionar los controles y activos de información y modelar amenazas que deben analizarse en la evaluación de riesgos. Los expertos en seguridad de la información pueden necesitar ser incluidos en el proceso para asegurar que el riesgo El análisis se realiza adecuadamente.

Resumen de evaluación de riesgos de nivel 1

Después de haber analizado un conjunto de riesgos, la organización de Nivel 1 comienza a comprender algunos conceptos. sobre análisis de riesgos:

1. Los controles CIS pueden ayudar a las organizaciones de nivel 1 a modelar amenazas comparando sus actuales prácticas a buenas prácticas conocidas. Los controles CIS identifican cada uno una forma de salvaguardar sistemas, por lo que a la inversa muestran dónde y cómo algo podría salir mal.
2. Una vez que los impactos se definen en términos de consecuencias aceptables, inaceptables y altas, respaldan un método muy rápido, consistente y simple para evaluar los riesgos.
3. Del mismo modo, cuando las probabilidades se definen utilizando términos fáciles de comunicar, como previsibilidad, los riesgos pueden ser fáciles de estimar a la vez que creíbles.
4. Si un riesgo puede ser evaluado de manera creíble como no previsiblemente creando un impacto, o previsiblemente creando un impacto aceptable, entonces una organización puede aceptar razonablemente ese riesgo.
5. Si un riesgo presenta una puntuación de riesgo más alta que otros riesgos, es probable que se priorice sobre otros riesgos durante el diseño y planificación del tratamiento de riesgos.

Recomendaciones de tratamiento de riesgos

Introducción

Las organizaciones a menudo piensan en las salvaguardas de seguridad como obstáculos para los negocios y la productividad. Las salvaguardas a menudo hacen que el personal tome medidas adicionales para acceder a los sistemas o la información, o para obtener la aprobación de las actividades comerciales normales. Las salvaguardas requieren inversiones en tiempo y dinero, que compiten con otras prioridades. Y si se vuelven demasiado perjudiciales para la misión, un misión de la organización, las salvaguardas de seguridad pueden ser desagradables y evitadas.

De hecho, las salvaguardias disruptivas a menudo hacen que el personal trabaje a su alrededor solo para obtener su trabajo hecho, lo que crea más riesgo.

Pero las recomendaciones de tratamiento de riesgo pueden y deben dar como resultado salvaguardas que sean demostrables razonable. Y mientras obtener una definición clara de "salvaguardas razonables" ha sido un desafío en las comunidades legales, regulatorias y de seguridad de la información, el CIS RAM proporciona un Solución práctica. Los evaluadores de riesgos evalúan las recomendaciones de tratamiento de riesgos para determinar si una salvaguarda de seguridad es razonable por; comparar la salvaguardia con el riesgo que se pretende reducir, y al comparar la salvaguarda con los criterios de aceptación del riesgo.

Las recomendaciones de tratamiento de riesgos son simples de evaluar una vez que los criterios de evaluación de riesgos y Se ha establecido un análisis de riesgo inicial. El proceso se realiza en los siguientes pasos:

1. Mientras examina un riesgo inaceptablemente alto, revise el Control CIS que corresponde con el riesgo y recomendar una forma factible para que la organización implemente o mejore ese controlar.
2. Si ese control no es factible en el corto plazo, recomiende otros controles CIS relacionados con El riesgo que se puede utilizar para reducirlo.
3. Evaluar el riesgo de la salvaguarda recomendada para comprender la carga que representaría a la organización. Luego compare ese riesgo de salvaguarda con los criterios de aceptación de riesgo para determinar si es apropiado
4. Compare también el riesgo evaluado de la salvaguarda recomendada con el riesgo observado para determinar si la salvaguarda es razonable (salvaguardas con puntajes de riesgo más bajos que los riesgos observados son razonables)
5. Clasifique los riesgos por su puntaje de riesgo para priorizar los riesgos y los tratamientos de riesgo que el la organización invertirá en

Esta sección muestra estos pasos en detalle al describir el proceso y luego al modelar el riesgo tratamientos para los riesgos inaceptablemente altos que se evaluaron en secciones anteriores.

El lector debe revisar las definiciones de 'razonable' y 'apropiado' que se proporcionan en el glosario. Estos términos se usarán regularmente en esta sección y tienen significados distintos.

1. Apropiado: una condición en la cual los riesgos para los activos de información no previsiblemente crearán daño que es mayor que la organización o sus constituyentes pueden tolerar.
2. Razonable: una condición en la cual las salvaguardas no crearán una carga para la organización eso es mayor que el riesgo contra el cual está destinado a proteger.

Objetivos de tratamiento de riesgos

El objetivo de las recomendaciones de tratamiento de riesgos bien formadas es crear una lista priorizada de salvaguardas de seguridad de la información que proporcionarían protecciones apropiadas mientras no posan demasiado Una gran carga para el propósito de la organización.

Los ejercicios de recomendación de tratamiento de riesgo que se demuestran en esta sección examinan el riesgos inaceptables que se ilustraron anteriormente en el documento y seleccionarán los Controles CIS que

Página 50

reduciría esos riesgos en un grado que sea razonable (no excesivamente pesado) y apropiado (no inaceptablemente dañino).

Recomendaciones de salvaguardas de tratamiento de riesgos de los controles CIS V7

A medida que examinamos riesgos inaceptablemente altos, recomendaremos salvaguardas basadas en CIS Controles V7. Pero algunas de las salvaguardas que una organización está preparada para implementar y operar no puede implementarse exactamente como se describe en CIS Controls V7. Este proceso lleva en cuenta cómo seleccionar controles que aborden los riesgos y cómo determinar si son diseñado de una manera que tenga sentido en el contexto tanto del riesgo como de la carga potencial para el organización.

Recuerde la relación entre los riesgos analizados y sus tratamientos de riesgo recomendados en la Figura 7)

Figura 7 - Balance dentro del análisis de riesgo central

Un riesgo y su salvaguarda propuesta se evalúan utilizando el mismo criterio. Si un propuesto la salvaguarda tiene un riesgo más alto (su "riesgo de salvaguarda") que los criterios de aceptación del riesgo, entonces no es apropiado. Si la salvaguardia tiene una puntuación más alta que el riesgo observado, entonces no es razonable.

Los ejercicios en esta sección se centrarán en hacer coincidir los análisis de riesgo completados (en azul) con los nuevos garantías recomendadas (en verde).

Ejemplo de tratamiento de riesgos 1 - CIS Control 1.1
El primer ejercicio que demostró el análisis de riesgos en la Tabla 23 mostró que la organización de Nivel 1 que su método para identificar e inventariar activos técnicos en su red no era suficiente. los El riesgo que representaba para la organización era demasiado alto.

Para recomendar una salvaguarda adecuada, la organización revisa la descripción de Control CIS 1.1 y consideran su objetivo. CIS Control 1.1 pretende que las organizaciones deberían activamente y haga un inventario pasivo de todos los sistemas IP que se unen a las redes de una organización para que sepan qué activos técnicos para incluir en sus programas de gestión de riesgos, salvaguardas, controles y procesos.

Se dan cuenta de que la mejor solución para ellos será comprar e instalar un dispositivo que identifica y cataloga activamente los hosts IP que se unen a la red, lo que permite al personal de TI agregar detalles información sobre cada activo a lo largo del tiempo. En este momento, no necesitan decidir cuál es la función completa El conjunto debería ser (es decir, funcionará como un dispositivo de control de acceso a la red para aplicar configuraciones seguras de sistemas, buscará activamente licencias de software, se integrará en un cambio base de datos de gestión o aplicación de mesa de servicio, etc.).

A continuación, evaluarán cuáles creen que son los riesgos de salvaguarda y determinarán si El riesgo de salvaguarda es apropiado o no. Este paso se demuestra en la Tabla 27.

Nota: El evaluador de riesgos registrará cómo abordarán su riesgo al indicar "Aceptar" “Reducir”, “Transferir” o “Evitar”. *Aceptar* y *reducir* riesgos será intuitivo para el lector. Un

la organización puede *transferir* un riesgo mediante la contratación de un tercero que puede manejar el riesgo mejor, o mediante adquirir una póliza de seguro contra el riesgo. La organización también puede *evitar* el riesgo por no participar más en los procesos o manejar los activos de información que causan el riesgo.

Tabla 27 - Ejemplo de riesgo para el control CIS 1.1

Análisis de riesgo	Valor
Control CIS	1.1
Descripción	Utilice una herramienta de descubrimiento activa para identificar dispositivos. conectado a la red de la organización. Esta herramienta deberá actualizar automáticamente el dispositivo de hardware de la organización inventario cuando se descubren dispositivos.
Activo de información	Todos los dispositivos.

Controlar	Los escaneos de vulnerabilidad ocurren ocasionalmente y pueden no identificar todos los sistemas que han estado en la red entre escaneos.
Vulnerabilidad	Sistemas que se han unido a la red entre esporádicos los escaneos no serán detectados.
Amenaza	Los hackers o malware pueden atacar y controlar sistemas que no han sido detectados, controlados y monitoreados.
Probabilidad de amenaza	2
Impacto de la misión	1
Obligaciones Impacto	3
Puntuación de riesgo	**6 6**
Aceptabilidad del riesgo	**Inaceptable**
Opción de tratamiento de riesgo	Reducir
Salvaguardia recomendada	Compre e implemente un dispositivo que activamente y identifica pasivamente los hosts IP en todas las redes. Implementar un proceso para agregar rutinariamente información sobre activos a El aparato. El dispositivo debería alertar opcionalmente sobre nuevos hosts que se unen a la red.
Salvaguardar el riesgo	Un costo moderado tendría un impacto mínimo en el presupuesto. La instalación de la herramienta probablemente no sea perjudicial. Costo moderado en tiempo del personal para agregar información sobre Activos IP a la base de datos del dispositivo. Después de establecer una línea de base, podremos distinguir entre sistemas de propiedad de la organización, y sistemas que no controlamos. Las alertas se pueden configurar después la línea de base está completa.
Salvaguardia Amenaza Probabilidad	1
Salvaguardar el impacto de la misión	1
Obligaciones de salvaguardia Impacto	3
Puntuación de riesgo de salvaguarda	**3**
Aceptabilidad del riesgo	**Aceptable**

Page 52

Revise los criterios de evaluación de riesgos y los criterios de aceptación de riesgos para la organización de Nivel 1 y Observe que la organización cree que con la salvaguarda recomendada, el riesgo ya no sería previsible.

La organización de Nivel 1 ha determinado que su salvaguarda recomendada es un dispositivo que puede identificar e inventariar hosts IP y alertar sobre nuevos hosts: es un método aceptable y razonable salvaguardia. El riesgo de salvaguardia estimado es menor que su nivel de riesgo aceptable y es menor. que el riesgo evaluado originalmente que está abordando.

Antecedentes: ¿qué tan realistas son las estimaciones de riesgo de salvaguarda?

Los lectores críticos se preguntarán cómo la organización y su asesor de riesgos sabrán si Sus estimaciones de riesgo de salvaguardia son realistas. Después de todo, ¿cómo pueden saber prospectivamente qué su riesgo estaría en tal situación?

Hay dos elementos importantes a tener en cuenta al obtener comodidad con esta práctica; Comprender las expectativas legales y regulatorias para la gestión de riesgos, y la información estándares de seguridad para evaluar las salvaguardas después de que se hayan implementado.

Ley y regulación: las leyes y regulaciones generalmente esperan que el análisis de riesgos evalúe salvaguardas que se requieren para lograr el cumplimiento, y se espera que el análisis de riesgos sea realizado por personas debidamente capacitadas e informadas. Estos análisis no garantizan

seguridad que es suficiente contra cualquier amenaza, pero proporcionan un plan para mejorar seguridad y cumplimiento que se prioriza por la probabilidad de daño, y que no tiene intolerable daño como su objetivo.

Normas de gestión de riesgos de seguridad de la información: evaluación de riesgos de seguridad de la información Los estándares en los que se basa la RAM CIS operan dentro de programas de gestión de riesgos más completos y ciclos ISO 27005 opera dentro de la familia de estándares ISO 27000, y NIST 800-30 funciona dentro de las publicaciones especiales del NIST. Cada una de estas familias de estándares requiere continua análisis de salvaguardas de seguridad, incluido el análisis de controles después de que se hayan implementado para determinar si son efectivos para abordar sus objetivos de seguridad. Recomendado por lo tanto, las salvaguardas deben evaluarse nuevamente después de la implementación para asegurarse de que lograr sus objetivos previstos.

Ejemplo de tratamiento de riesgos 2 - Control CIS 3.4

El segundo análisis de riesgos de la organización de Nivel 1 incluyó su método para identificar y abordar parches del sistema en su entorno de producción y su entorno corporativo. Se sentían cómodos con su proceso de gestión de parches en su entorno de producción. A pesar de que no estaban utilizando el control descrito en CIS Control 3.4 como estaba escrito, ellos estimó que la probabilidad y el impacto del riesgo de que sus métodos actuales los expongan a cumplió un nivel de riesgo aceptable.

Sin embargo, sus riesgos en el entorno corporativo eran mayores. Su gestión empresarial la aplicación tenía vulnerabilidades para las que el fabricante no podía proporcionar parches, pero esperaba para abordar las vulnerabilidades conocidas en una versión importante pronto. La organización creía que el la actualización de lanzamiento sería significativamente perjudicial a corto plazo, y esperaba encontrar un salvaguarda alternativa que sería razonable y apropiada. Entonces la organización modelará tratamientos de riesgo recomendados en la Tabla 28 para identificar tal salvaguarda.

Sabiendo que no podían implementar CIS Control 3.4 como está escrito, consideran el objetivo de el control en su lugar para ver si hay medios alternativos para cumplir el objetivo. Ellos determinan que CIS Control 3.3 pretende que los parches se apliquen lo más rápido posible, lo cual no es

Page 53

factible en este caso. Debido a que CIS Control 3.3 no es factible, recurren a otros controles CIS para ver qué alternativas están disponibles para ellos.

El CIS ® proporciona un documento titulado *CIS Community Attack Model* [16] que puede ser útil para organización para encontrar controles alternativos. El modelo de ataque comunitario (proporcionado en el *CIS_RAM_Workbook* en una pestaña titulada "Modelos de ruta de ataque" y en el sitio web de CIS) asocia el CIS controla la forma en que reducen los riesgos en cada etapa de un incidente en función de las funciones encontrado en el NIST Cybersecurity Framework. [17] Esto puede ser muy útil para identificar relacionados controles.

Figura 8 - Modelo de ataque comunitario parcial

Los evaluadores de riesgos pueden hacer referencia al Modelo de ataque comunitario para encontrar controles que puedan ser complementarios y alternativos a las salvaguardas recomendadas que están evaluando. Si una la organización lucha por implementar un subcontrol, podrían buscar controles que jueguen de manera similar papel en el Modelo de ataque comunitario para encontrar controles alternativos que puedan ayudarlos a cumplir con el mismo objetivo de seguridad. Por ejemplo, si una organización no puede usar fácilmente los registros de auditoría para *detectar entrega* de un tipo de amenaza, pueden buscar otro control en la celda que se cruza con el

[16] Se puede acceder al *Modelo de ataque comunitario* aquí: https://www.cisecurity.org/white-papeles / modelo de ataque comunitario cis /

[17] *Marco para Mejorar la Ciberseguridad de Infraestructura Crítica, Versión 1.0* , Instituto Nacional de Estándares y tecnología. 12 de Febrero de 2014

Page 54

detectar la fila y la columna de *entrega* para encontrar controles similares, y eventualmente ver la red controles de detección de intrusos, que pueden ser más útiles en su entorno.

Dada la intención del CIS Control 3 (del cual CIS Control 3.4 es miembro) para realizar evaluaciones de vulnerabilidad, el evaluador de riesgos revisa el Modelo de ataque comunitario y encuentra "Evaluación continua de vulnerabilidad" en múltiples ubicaciones. Parece ser útil para *proteger* contra el *reconocimiento inicial* , la *protección* contra la *entrega* y la *protección* contra el *mal uso / escalar Privilegio* (así como otros usos que se muestran en el resto del modelo no visible en Figura 8).

La amenaza que intentan abordar podría mitigarse *protegiendo* el sistema en el momento de la *entrega* , y para evitar que los atacantes y el malware sepan qué vulnerabilidades están presentes. Entonces el riesgo el evaluador considera la posibilidad de sistemas de prevención de intrusiones en la red (NIPS) y se refiere a CIS Control 12 para "Defensa de límites" para ver cómo se describe eso. Mientras revisa el control CIS Sub-controles de 12, se encuentran con CIS Control 12.7 y ven una descripción para una intrusión sistema de prevención (IPS) que podría ser apropiado para su riesgo. Un IPS podría detectar y prevenir acciones que hacen coincidir exploits con vulnerabilidades conocidas. Otras opciones, como poner la empresa la planificación de la aplicación y sus usuarios en una VLAN separada podría reducir la probabilidad de un ataque a medida que bueno, pero habría muchos sistemas en esa VLAN, por lo que la reducción de probabilidad podría ser pequeña.

Recomiendan y evalúan una salvaguarda basada en el Control CIS 12.7.

Tabla 28 - Ejemplo de riesgo para el control CIS 3.4

Análisis de riesgo	Valor
Control CIS	3.4
Descripción	Implemente herramientas de actualización de software automatizadas para garantizar que los sistemas operativos están ejecutando los más recientes actualizaciones de seguridad proporcionadas por el proveedor del software.
Activo de información	Aplicación de gestión empresarial en el interno red corporativa.
Controlar	Los análisis de vulnerabilidad se producen cuando el Servicio de información sobre amenazas anuncia una vulnerabilidad de moderada a alta que necesita parches El equipo parchea la mayoría de los sistemas dentro de las 24 horas de anuncio.
Vulnerabilidad	Los sistemas de aplicaciones de gestión empresarial son

Amenaza	Sin parche por más de un año. Los piratas informáticos o el malware pueden atacar y controlar la empresa entorno de aplicación de gestión.
Probabilidad de amenaza	2
Impacto de la misión	2
Obligaciones Impacto	3
Puntuación de riesgo	**6 6**
Aceptabilidad del riesgo	**Inaceptable**
Opción de tratamiento de riesgo	Reducir
Salvaguardia recomendada	(Control CIS 12.7) Comprar e implementar un IPS solución para detectar, alertar y prevenir ataques al

Página 55

Análisis de riesgo	Valor
	aplicación de gestión empresarial y otros vulnerables sistemas en el medio ambiente.
Salvaguardar el riesgo	Un costo significativo tendría un impacto significativo en el presupuesto. La instalación de la herramienta en modo de detección es probable No es perjudicial. La instalación de la herramienta en modo de prevención es Probablemente perjudicial. Costo moderado en tiempo de personal para implementar y configurar el sistema IPS.
Salvaguardia Amenaza Probabilidad	3
Salvaguardar el impacto de la misión	2
Obligaciones de salvaguardia Impacto	1
Puntuación de riesgo de salvaguarda	**6 6**
Aceptabilidad del riesgo	**Inaceptable**

El uso de una protección basada en CIS Control 12.7 en esta implementación planificada todavía se evalúa como inaceptable. El evaluador de riesgos está seguro de que el IPS en términos de presupuesto y posible interrupción de servicio evitará que la organización atienda adecuadamente a algunos de sus usuarios pacientes población (Probabilidad = '3'; Impacto de la misión = '2'; Puntuación de riesgo de salvaguarda = '6'). Para un nivel 1 organización especialmente, implementar una herramienta que pueda crear interrupciones en los negocios sería intolerable, y probablemente conduciría a una mayor frustración por la gestión no técnica con seguridad de información.

Entonces, el evaluador de riesgos considera implementar un IPS de código abierto en modo de detección y alerta (Sistema de *detección de* intrusiones o IDS), en lugar de un IPS comercial en modo de prevención. Esta permitiría al equipo estar al tanto de actividades sospechosas y responder sin crear una falla de funciones comerciales. Después de familiarizarse y sentirse cómodo con el IPS y ver qué acciones que alerta, el equipo de tecnología puede bloquear selectivamente el acceso a personas de alto riesgo sistemas, como el sistema de gestión empresarial.

Encuentran un Control CIS correspondiente después de revisar los subcontroles en el Control 12 CIS. el evaluador de riesgos lee CIS Control 12.6 que dice: "Implemente la detección de intrusiones basada en la red Sensores de sistemas (IDS) para buscar mecanismos de ataque inusuales y detectar el compromiso de estos sistemas en cada uno de los límites de la red de la organización ". Este control puede ser el inicial salvaguarda, lo que permite a la organización mejorar la salvaguarda de un IPS (CIS Control 12.7) cuando la organización está lista para bloquear el tráfico que entienden mejor.

La Tabla 29 modela una variación de esta protección recomendada.

Tabla 29 - Ejemplo de recomendación de tratamiento de riesgos Control CIS 12.6 para reducir el riesgo Control CIS 3.4.

Análisis de riesgo	Valor
Opción de tratamiento de riesgo	Reducir
Salvaguardia recomendada	(Control CIS 12.7) Adquirir e implementar un código abierto Solución IPS para detectar y alertar sobre ataques en el aplicación de gestión empresarial y otros vulnerables

Page 56

Análisis de riesgo	Valor
	sistemas en el medio ambiente. Después de ganar confianza en el tipos de acciones y alertas detectadas, despliegue la capacidad IPS para proteger sistemas de alto riesgo.
Salvaguardar el riesgo	Costo moderado en tiempo de personal para implementar y configurar el sistema IPS.
Salvaguardia Amenaza Probabilidad 3	
Salvaguardar el impacto de la misión	1
Obligaciones de salvaguardia Impacto	1
Puntuación de riesgo de salvaguarda 3	
Aceptabilidad del riesgo	**Aceptable**

El asesor está seguro de que el impacto en la misión y las obligaciones no se verán afectadas utilizando IPS como IDS (en modo de detección versus modo de prevención). En este punto, el evaluador de riesgos es confía en que tienen un plan para implementar una salvaguarda que se alinee con el Control CIS 12.6 eso reduciría el riesgo evaluado por su revisión de CIS Control 3.4.

Ejemplo de tratamiento de riesgos 3 - Control CIS 14.9

Finalmente, el análisis de riesgos de la organización de Nivel 1 que involucra el Control 14.9 de CIS mostró una inaceptable riesgo de cómo registraron eventos en la aplicación de gestión empresarial. Dada su preocupación se da cuenta de que se espera que los empleados descontentos roben y abusen de datos en el medio ambiente deberán rastrear el acceso a la aplicación y recibir alertas sobre acciones específicas, como descargas de datos

La organización sabe que los sistemas de gestión de registros y los SIEM se pueden implementar fácilmente como los servicios y la administración serían más amigables para detectar abusos de acceso que invertir en aspectos más esotéricos de la prevención de intrusiones. Entonces optan por recomendar un SIEM-as-Solución de servicio para abordar este riesgo.

Tabla 30 - Ejemplo de recomendación de tratamiento de riesgos para el control CIS 14.9

Análisis de riesgo	Valor
Control CIS	14,9
Descripción	Aplicar registros de auditoría detallados para acceder a datos confidenciales o cambios en datos confidenciales.
Activo de información	Aplicación de gestión empresarial
Controlar	Los registros de acceso se capturan y almacenan localmente, y no revisados.
Vulnerabilidad	La organización no tiene conocimiento de sospechas o inapropiados. utilizar.
Amenaza	Empleados no autorizados o hackers que usan privilegios escalados y puede acceder y abusar de información no pública en el solicitud.

57

Análisis de riesgo	Valor
Probabilidad de amenaza	3
Impacto de la misión	2
Obligaciones Impacto	3
Puntuación de riesgo	**9 9**
Aceptabilidad del riesgo	**Inaceptable**
Opción de tratamiento de riesgo	Reducir
Salvaguardia recomendada	Implementar un SIEM como servicio. Para evitar ser abrumado por mensajes de registro y alertas, enfóquese primero a SIEM en sistemas de alto riesgo, como la gestión empresarial solicitud. Alerta sobre cualquier manipulación de datos y descargas realizado por cuentas de administrador.
Salvaguardar el riesgo	La sintonización inicial puede ser un desafío, pero no interferirá con Nuestra misión u obligaciones.
Salvaguardia Amenaza Probabilidad	2
Salvaguardar el impacto de la misión	1
Obligaciones de salvaguardia Impacto	1
Puntuación de riesgo de salvaguarda	**2**
Aceptabilidad del riesgo	**Aceptable**

La organización ahora está segura de que sus recomendaciones de tratamiento de riesgos son razonables y apropiado, a pesar de que los planes no incluyen una implementación completa de todos los CIS Controles a todos los activos dentro del alcance.

Además, la organización sabe que tienen una base para explicar y defender su plan para partes interesadas y autoridades, y defender la base por la cual aceptan ciertos riesgos.

Ejercicio :

El lector debe usar la plantilla Registro de riesgos - Nivel 1 que se proporciona en el documento complementario *CIS_RAM_Workbook* para ingresar recomendaciones de tratamiento de riesgo para cada riesgo evaluado como inaceptablemente alto.

El lector debe considerar:

1. Si se puede mejorar una salvaguarda existente y cómo se haría.
2. Si una salvaguarda basada en un Control CIS diferente proporcionaría riesgo apropiado
3. Colaborar con expertos en temas de seguridad de la información para ayudar a modelar eficacia potencial de las salvaguardas recomendadas.

El evaluador de riesgos necesitará usar su juicio profesional para diseñar y recomendar salvaguardas de seguridad de la información y evaluar prospectivamente el riesgo que pueden presentar.

58

Los expertos en seguridad de la información pueden necesitar ser incluidos en el proceso para asegurar que el riesgo El análisis se realiza adecuadamente.

Resumen de recomendaciones de tratamiento de riesgos

Las recomendaciones de tratamiento de riesgos son una parte crítica de las evaluaciones de riesgos para garantizar que La organización ha desarrollado un plan para abordar los riesgos sin crear otros riesgos para el organización o sus constituyentes. Algunos de los beneficios que se han demostrado sobre esto proceso son:

1. Las organizaciones pueden demostrar a los gerentes de negocios colaboradores cómo se recomienda se pueden implementar salvaguardas de seguridad sin crear demasiada carga para el misión comercial
2. Las organizaciones pueden demostrar a los reguladores y otras autoridades legales que las salvaguardas son razonables porque el riesgo de la salvaguardia (la "carga" para la organización) no es mayor que el riesgo que se pretende reducir.
3. Las organizaciones pueden demostrar que las salvaguardas recomendadas serían apropiadas mostrando que previsiblemente no crearían un impacto que sería intolerable para el organización o sus constituyentes.

El proceso para evaluar riesgos y recomendar tratamientos de riesgo apropiados ha sido demostrado a nivel general. Sin embargo, algunas preguntas probablemente permanezcan para el lector sobre evaluar salvaguardas, estimar probabilidad y la idoneidad de modelos de probabilidad en riesgo análisis. Estos temas más detallados se analizarán en el próximo capítulo "Análisis de riesgos Técnicas.

Capítulo 3: Evaluación de riesgos basada en activos

Instrucciones para organizaciones de nivel 2

Las instrucciones de evaluación de riesgos del **Nivel 2** son adecuadas para organizaciones que se ajustan al perfil del Nivel 2 organizaciones según lo descrito por el NIST Cybersecurity Framework **.** Estas organizaciones pueden ser identificado por tener las siguientes características:

- **Nivel NIST** : organizaciones de Nivel 2. Los materiales de nivel 2 son los más adecuados para organizaciones que tener al menos alguna colaboración con la gerencia comercial no técnica para definir el riesgo criterios
- **Experiencia** : la organización tiene recursos y capacidades para analizar la seguridad común amenazas y planificar salvaguardas apropiadas para el riesgo. Sin embargo, no tienen a la mano habilidades para modelar cómo operarían las amenazas dentro de su organización.
- **Tiempo** : la organización puede invertir suficiente tiempo para analizar los riesgos a nivel de sistemas, dispositivos y aplicaciones específicos, y subcomponentes dentro de esos activos.

Este capítulo consta de secciones que abordan cada una de las actividades específicas dentro de un riesgo. evaluación. Los lectores deben participar en este capítulo leyendo primero el texto en cada sección, y luego realizar los ejercicios que se recomiendan para cada sección. El material presentado en la RAM CIS es sustancialmente diferente de muchos otros estándares y modelos de evaluación de riesgos, así que el lector primero debe comprender el objetivo de cada sección y luego practicar lo que aprende utilizando plantillas que se proporcionan en el documento complementario *CIS_RAM_Workbook* .

Al realizar su primera evaluación de riesgos basada en RAM CIS, las organizaciones deben tener cuidado de no trate de "hervir el océano". Los organismos reguladores y las normas de seguridad de la información entienden por igual que no todos los riesgos pueden identificarse en una sola evaluación. Las organizaciones deben continuamente y Evaluar regularmente los riesgos para identificar, comprender y gestionar los riesgos a lo largo del tiempo.

El proyecto de evaluación de riesgos

Visión general

Las evaluaciones de riesgos son proyectos con pasos claros para preparar, conducir y reportar riesgos análisis. Y aunque los proyectos de evaluación de riesgos se pueden modelar con un plan típico, cada El enfoque del proyecto de la organización variará dependiendo de factores como la disponibilidad de recursos y se desarrollará con el tiempo a medida que las organizaciones se vuelvan más capaces en su madurez de ciberseguridad. Esta La sección describirá un proyecto de evaluación de riesgos, sus componentes y variaciones, y presentará orientación para preparar el plan.

El esquema del proyecto

Las evaluaciones de riesgos se realizan utilizando una serie de pasos que incluyen acciones típicas y roles como se muestra en la Tabla 31.

Tabla 31 - Ejemplo de esquema de proyecto de evaluación de riesgos

Paso	Tarea	Papeles clave
1	Definición del alcance y programación de sesiones	Ejecutivos, Gerentes, Asesores
2	Definición de criterios de evaluación de riesgos	Gerente, Asesor
3	Definición de criterios de aceptación de riesgos	Ejecutivos, Gerencia, Asesor
4 4	Evaluación de riesgos (basada en activos)	
4.1	Reunir evidencias	Personal, Gerencia, Asesor
4.2 4.2	Modelar las amenazas	Personal, Gerencia, Asesor

Paso	Tarea	Papeles clave
4.3 4.3	Evaluación de riesgo	Asesor
5 5	Proponer salvaguardias	
5.1	Evaluar las salvaguardas propuestas	Asesor, Gerencia

Durante el **Paso 1** (Definición del alcance y las sesiones de programación), la organización determinará qué activos de información para incluir en su evaluación. También identificarán dueños de negocios y delegados técnicos que proporcionarán pruebas y entrevistas para evaluar esos activos. El riesgo El asesor luego programará sesiones de entrevistas con esos propietarios y delegados.

En el **Paso 2** (Definición de criterios de evaluación de riesgos), la organización definirá las reglas mediante las cuales

evaluar y puntuar riesgos. Definirán su misión (el valor que aportan a los demás), su objetivos (sus definiciones organizacionales para el éxito y el fracaso), y sus obligaciones (el potencial de daño contra otros) para establecer lo que están tratando de proteger. Luego definirán esquemas de puntuación que se utilizarán para la estimación de impacto y probabilidad.

En el **Paso 3** (Definición de criterios de aceptación de riesgos) la organización establecerá su tolerancia al riesgo mediante seleccionar una combinación de la probabilidad de un impacto que sería tolerable para todas las partes (el organización y partes que pueden verse perjudicadas por los riesgos realizados).

En el **Paso 4** (Evaluación de riesgos - Basado en activos) el evaluador de riesgos evaluará los riesgos de activos de información. Para las organizaciones de nivel 2, el análisis incluye las siguientes actividades:

- "Recopilar evidencia" implica una revisión de documentos, como políticas, procedimientos, normas y puntos de referencia. También incluye entrevistas con la gerencia y el personal. La recopilación de evidencia también implica la observación de configuraciones, artefactos, instalaciones, registros, y procesos de trabajo para determinar si operan de manera segura o vulnerable. Los niveles de recopilación de evidencia estarán directamente asociados con la madurez de la organización.
- En la actividad "Modelar las amenazas", la organización modelará los riesgos con al menos estos componentes; Controles de CIS que deberían estar en su lugar para proteger los activos de información, salvaguardas que protegen efectivamente los activos de información según lo descrito por los Controles CIS, y vulnerabilidades que resultan si las salvaguardas no son suficientemente efectivas. El orden en que estos componentes se consideran depende de la madurez de la organización, como se describirá más adelante en este documento.
- Durante la "Evaluación de riesgos", la organización estimará la probabilidad y el impacto de la riesgos Las estimaciones se basarán en la puntuación y los criterios establecidos en Paso 2. La puntuación de riesgo se calculará automáticamente para determinar si el actual Las implementaciones de los controles CIS ya son razonables.

Durante el **Paso 5** (Proponer salvaguardas), la organización considerará cómo abordar los motivos irrazonables riesgos seleccionando controles CIS que deben implementarse para abordar cada riesgo, y específicamente cómo se implementarán los controles. Estas salvaguardas pueden incluir dispositivos de seguridad, físicos salvaguardas, capacitación, procesos de supervisión u otros métodos. El evaluador de riesgos luego evaluará el razonabilidad de las salvaguardas durante "Evaluar las salvaguardas propuestas". El evaluador de riesgos evaluar las salvaguardas propuestas utilizando los mismos criterios que se usaron para evaluar los riesgos.

Una plantilla de plan de proyecto está disponible en el documento complementario *CIS_RAM_Workbook* .

Definición del alcance y la programación de sesiones

Nota: El lector debe usar las hojas de trabajo proporcionadas en el documento complementario. CIS_RAM_Workbook mientras lee estas instrucciones. El lector comprenderá mejor el conceptos y su uso practicando los métodos descritos en este capítulo.

Página 61

Definiendo el Alcance

Las organizaciones deben realizar evaluaciones de riesgos con un alcance de información claramente definido bienes. Un tema único generalmente limita el alcance de los activos, como "activos de información que contienen información confidencial "," el centro de datos "," áreas y tecnologías de práctica de ingeniería que los respaldan "o una división comercial específica.

Si bien es posible seleccionar activos de información no relacionados para una evaluación, o un subconjunto de activos dentro de un alcance mayor: la organización que recibe la evaluación y está haciendo las inversiones y las decisiones de priorización basadas en sus hallazgos serán más cómodas cuando los activos de información están asociados con una entidad comercial o un proceso comercial. De lo contrario, riesgo Los resultados de la evaluación pueden parecer dispersos y no relacionados.

Del mismo modo, al evaluar el riesgo de un conjunto de activos de información, tiene sentido considerar Un conjunto de activos que pueden afectar directamente la seguridad de los demás. Por ejemplo, una evaluación de riesgos que examina un conjunto de aplicaciones que también deben incluir los dispositivos de red que conectan aplicaciones a otros activos y otras redes, así como los procesos que se utilizan para desarrollar y gestionar esas aplicaciones. Estos sistemas están directamente conectados entre sí y dependen unos de otros por lo que sus riesgos se asocian fácilmente entre sí.

Las organizaciones no pueden examinar todos los activos de información de manera integral en un solo riesgo evaluación, por lo que su alcance debe considerar el tiempo y los recursos disponibles para

evaluación . Los evaluadores de riesgos deben consultar a expertos en seguridad para ayudarlos a determinar qué activos, amenazas y riesgos a priorizar.

Una tabla de alcance de ejemplo (Tabla 32) demuestra el nivel de detalle apropiado para un plan de evaluación inicial y se proporciona en el libro de trabajo *CIS_RAM_Workbook.*

Tabla 32 - Tabla de alcance de ejemplo

Tipo de activo	Nombre de activo	Propietario de la empresa	Mayordomo
Información	Código de aplicación	ARRULLO	CIO
Información	Información del paciente	Experiencia del cliente	CIO
Solicitud	Registro de pacientes (prod)	Experiencia del cliente	Gerente de producto
Solicitud	Registro de patentes (dev)	Experiencia del cliente	Desarrollo de software
Solicitud	DataMart	Departamento de Innovaciones	DevOps
Servidor	ProductionAppSrvr1	Experiencia del cliente	DevOps
Servidor	ProuctionDBServer2	Experiencia del cliente	DevOps
Servidor	DevAppSrvr1	Desarrollo de software DevOps	
Servidor	DevDBServer2	Desarrollo de software DevOps	
Servidor	LDAP1	CIO	DevOps
Servidor	DNS1	CIO	DevOps
Router principal de dispositivo de red		CIO	Ingeniería en Redes
Dispositivo de red Enrutador DMZ		CIO	Ingeniería en Redes
Dispositivo de red Firewall 1		CIO	Ingeniería en Redes
Dispositivo de red Firewall 2		CIO	Ingeniería en Redes
Conmutador de dispositivo de red		CIO	Ingeniería en Redes
Proceso	AppDev	Experiencia del cliente	Desarrollo de software
Proceso	Promoción de código	Experiencia del cliente	DevOps
Proceso	Mantenimiento	Gerente de producto	DevOps

Page 62

Tipo de activo	Nombre de activo	Propietario de la empresa	Mayordomo
Proceso	Gestión del cambio	Gerente de producto	DevOps
Proceso	Gestión de vulnerabilidades	CIO	Equipo de seguridad
Proceso	Configuracion de cuenta	Experiencia del cliente	Gestión de aplicaciones
Proceso	Mantenimiento de la cuenta	Experiencia del cliente	Gestión de aplicaciones
Proceso	Experiencia de cliente de incorporación de nuevos clientes		Gestión de aplicaciones
Proceso	Auditoría interna	Conformidad	Auditoría interna
Proceso	Configuración del dispositivo / sistema	CIO	DevOps
Proceso	Atención al cliente	Experiencia del cliente	Gestión de aplicaciones

Tenga en cuenta que la tabla de alcance incluye los roles de propietario de negocio y los roles de administrador. Negocio los propietarios son los (normalmente) gerentes no técnicos responsables de la información y procesa que los activos de información soportan. Los delegados son (típicamente) gerentes técnicos que son responsable de la funcionalidad y seguridad de los activos de información. Al identificar información propiedad de activos por adelantado, la tabla de alcance se puede utilizar para ayudar a planificar sesiones de entrevista para resto de la evaluación de riesgos.

Independientemente de cómo se establezca el alcance de la evaluación de riesgos y de qué tan detallado sea el activo el listado es, hay algunas prácticas útiles que una organización debe tener en cuenta al identificar sus activos de información:

- Piense en un conjunto de activos ubicados de manera similar como una sola clase de activos. Por ejemplo, todos servidores de bases de datos que usan la misma tecnología y el mismo mantenimiento y Los métodos de administración pueden considerarse una clase de activo. Sin embargo, si un conjunto de los servidores de bases de datos son diferentes de otros (por ejemplo, contienen información confidencial en

una DMZ mientras que otros procesan información menos sensible en otra zona), estos pueden ser consideró dos activos porque sus riesgos serán diferentes, incluso si se administran idénticamente

- Los activos de información no son solo tecnologías que almacenan y transmiten información confidencial. Los activos de información son cualquier información, tecnología, proceso, personas o instalaciones que puedan impactar la confidencialidad, integridad o disponibilidad de información.
- Incluir en el alcance todos los activos de información que están dentro de las mismas zonas (redes, instalaciones, etc.) como cualquier otro activo de información dentro del alcance.

El lector debe desarrollar su propia tabla de alcance utilizando la plantilla de tabla de alcance en el documento complementario *CIS_RAM_Workbook* .

Page 63

Ejercicio :

El lector debe desarrollar su propia tabla de alcance utilizando la hoja de trabajo "Alcance - Nivel 2" que está proporcionado en el documento complementario *CIS_RAM_Workbook.*

El lector debe considerar:

1. Un conjunto de activos de información que su organización está interesada en enfocar su seguridad recursos en?
    a. Este conjunto puede definirse por procesos, tecnologías, una clase de información o una localización.
2. ¿Cuáles son los límites entre este conjunto de activos de información y otra información? activos que no están en este alcance?
    a. Qué sistemas, instalaciones y dispositivos de red vinculan estos límites, o separarlos?
    si. ¿Se incluyen o excluyen estos activos "límite" del alcance?
3. Enumere los activos de información o las clases de activos que están dentro del alcance.
    a. Enumere los activos de información o las clases de activos con un nivel de detalle que el La organización tiene el tiempo y los recursos para analizar. Esto puede requerir ajuste durante el curso de la evaluación si la organización se da cuenta tiene más tiempo (o menos tiempo) de lo que originalmente planearon para evaluar activos de información.

Programación de sesiones de entrevista

Las sesiones de entrevista serán de actualidad y deberán abordar un tema o temas estrechamente relacionados para cada conversacion. Las sesiones de entrevista pueden centrarse en los controles CIS, o en los activos de información y activos clases

Por ejemplo, las sesiones de entrevistas que se centran en los controles de CIS reunirían al personal y gerencia que sabe cómo se implementa y opera cada control. Una sesión puede ser dedicado a CIS Control 1 para comprender cómo se inventarian los dispositivos. Otro puede ser programado para discutir el Control 2 de CIS para comprender qué salvaguardas existen para el inventario software. O, si el mismo personal conoce ambas salvaguardas, entonces quizás una sesión podría combinar ambos temas.

Del mismo modo, si los evaluadores de riesgos programan sesiones en torno a activos de información o clases de activos, entonces sería apropiado incluir dueños de negocios y dueños técnicos de esos sistemas para
Comprenda cómo se aplican los controles CIS asociados a cada activo o clase de activo.

Una sesión de ejemplo para una aplicación web puede incluir gerentes de producto, desarrolladores de aplicaciones, administradores de aplicaciones y dueños de negocios. Los temas en esa sesión pueden incluir el Control CIS 14, "Acceso controlado basado en la necesidad de saber", CIS Control 16, "Monitoreo de cuentas y Control "y CIS Control 18," Seguridad del software de aplicación ".

La forma en que la organización agrupa y ordena estos temas depende en gran medida de ellos, pero los evaluadores de riesgos debe tener en cuenta estos consejos al programar sesiones de entrevista:

1. Sea respetuoso con el tiempo de las personas. Si bien es importante recopilar información completa acerca de los riesgos, las organizaciones no pueden recopilar toda la información relevante en el primer o segundo riesgo evaluaciones
2. Trabajar con los gerentes para determinar la forma más eficiente y útil de programar entrevistas, ya sea por CIS Controls o por activos de información y clases de activos.
3. Espere que algunas salvaguardas de seguridad se apliquen de manera diferente a información diferente activos y clases de activos. Por ejemplo, CIS Control 5, "Configuración segura para

Página 64

Hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores "y CIS El control 16, "Monitoreo y control de cuentas" puede implementarse y supervisarse de manera diferente para servidores en diferentes entornos, o puede ser controlado centralmente para servidores, pero controlado individualmente para dispositivos de red. Planee evaluar cómo estos y otros similares Las salvaguardas se aplican a diferentes clases de activos.
4. Proporcione una agenda para la entrevista de alcance para ayudar a los participantes a preparar cualquier material o información sobre los activos o controles de información que pueden discutirse.

Programación de revisiones de evidencia
Los evaluadores de riesgos utilizan sesiones de revisión de evidencia para examinar los activos de información y; determinar si se ajustan a los controles de la CEI y evalúan si serían eficaces contra amenazas previsibles

Las sesiones de revisión de evidencia deben programarse después de las entrevistas para que el riesgo los evaluadores entienden el panorama general del entorno de seguridad antes de intentar Comprenda por qué ciertos activos están configurados de la forma en que están.

Durante las entrevistas, el evaluador de riesgos aprenderá sobre temas que deberían ser más cercanos entendido a través de una revisión de configuraciones, pruebas del sistema o revisión de registros. Evaluadores de riesgos deben tener en cuenta durante o poco después de la entrevista qué garantías querrán examinar más a fondo, e informar a los participantes que probablemente serán contactados más tarde en la evaluación para participar en esas sesiones de revisión de evidencia. Además, el asesor debe preguntar qué personal, procesos o activos de información serían apropiados para examinar para reunir evidencia. Las sesiones de revisión de evidencia se pueden programar al final de la entrevista.

Las técnicas para revisar la evidencia de la efectividad de los controles se presentan más adelante en el capítulo "Técnicas de análisis de riesgos".

Definición de criterios de evaluación de riesgos

Introducción

Los criterios de evaluación de riesgos son las declaraciones numéricas y en lenguaje sencillo que una organización utiliza para evaluar su riesgo de ciberseguridad. La forma más familiar de cálculos de riesgo, "Riesgo = Probabilidad x Impacto "es la base para el análisis de riesgos en la RAM CIS. Pero es solo el punto de partida para el análisis de riesgos.

Los criterios de evaluación de riesgos deben ser significativos para las organizaciones que los utilizan, por lo que deben ser vinculado al beneficio y daño potencial que la organización puede crear. El impacto de un La violación de la seguridad cibernética puede dañar a la organización misma, puede dañar la capacidad de la organización para cumplir con éxito su misión, o puede dañar a otros.

Debido a que las fallas de ciberseguridad impactan a las partes dentro y fuera de una organización, el riesgo Los criterios de evaluación deben ser universalmente significativos y deben abordar los intereses de todos partes potencialmente afectadas. Además, los criterios de evaluación de riesgos deben demostrar a las autoridades,

tales como reguladores y litigantes, que la organización considera el riesgo de daño a otros como tanto como el riesgo de daño a sí mismos.

Si bien estos requisitos pueden parecer complejos, el método presentado en esta sección Abordarlos suficientemente utilizando una técnica que sea fácil de desarrollar y usar.

Criterios de evaluación de riesgos Fundamentos

El análisis de riesgos proporcionado en el CIS RAM es, en su raíz, una cuestión de equilibrio entre el potencial de daños futuros contra la cierta carga de una salvaguardia. Los reguladores y litigantes tienen

Página 65

durante mucho tiempo consideró este equilibrio como clave para actuar como una "persona razonable". La estructura central de un La declaración de riesgo se proporciona a continuación para ilustrar el concepto central de equilibrio.

Figura 9 - Balance dentro del análisis de riesgo básico

Observe algunas cosas de inmediato con el modelo de análisis de riesgos en la Figura 9.

- Si bien las organizaciones generalmente evalúan el riesgo observado para determinar si deberían abordarlo o aceptarlo, esta declaración de riesgo compara deliberadamente el riesgo observado con un salvaguarda propuesta.
- El criterio que evalúa el riesgo también evalúa la salvaguarda.
- El impacto del riesgo estima el potencial de daño para la organización y el daño potencial contra otros.

Los evaluadores de riesgos comparan los riesgos con sus salvaguardas propuestas para determinar si las salvaguardas crearían un riesgo previsiblemente menor que el estado actual. Para lograr esto, el el evaluador evalúa el riesgo estatal actual (o "riesgo observado") y la salvaguarda propuesta utilizando Los mismos criterios para garantizar la comparabilidad.

Esta comparación evita que las organizaciones implementen salvaguardas excesivamente pesado, o que crea nuevos riesgos inaceptables. Por ejemplo, una organización que usa software que ya no es compatible con el proveedor, pero depende de ese software para negocios críticos propósitos, deben encontrar métodos alternativos para identificar y controlar posibles riesgos de seguridad hasta que reemplacen el software. Si la gerencia recomienda cambiar rápidamente a inferior, pero software seguro, la organización puede sufrir un mayor impacto en su misión que la seguridad riesgo que están tratando de evitar.

Al considerar CIS Control 18: Seguridad del software de aplicación, se puede hacer una declaración de riesgo para estimar la previsibilidad de una amenaza impactante. El riesgo puede establecerse tal como aparece en la Tabla 33 (donde el puntaje de riesgo '12' es un producto de la probabilidad '3' y el puntaje de impacto más alto '4'):

Tabla 33 - Ejemplo de declaración de riesgo central

Riesgo observado	Impacto de probabilidad de	Nosotros	Impactar a Otros	Riesgo Puntuación
Los hackers pueden explotar a los no compatibles, Pero aplicación crítica.	3	3	4 4	**12**

Un evaluador de riesgos debería recomendar y evaluar una salvaguarda para reducir la alta seguridad riesgo, como se ilustra en la Tabla 34. Aquí, la organización se daría cuenta de que la probabilidad de un El impacto negativo para su misión es mayor que el riesgo estatal actual. Este es un caso obvio de la carga es mayor que el riesgo y una salvaguarda recomendada no es razonable.

Página 66

Tabla 34 - Ejemplo de salvaguarda propuesta irrazonable

Propuesto Salvaguardia	Nuevo riesgo	Probabilidad	Impactar a Nosotros	Impactar a Otros	Salvaguardia Riesgo
Reemplazar aplicación con inferior, Aplicación segura.	La solicitud será funcionar ineficientemente	5 5	3	1	**15**

Cuando se enfrenta a este análisis, la organización debe encontrar otra forma de abordar el riesgo. Este proceso se describirá más adelante en este capítulo en la sección Tratamiento de riesgos Recomendaciones

Pero lo que debería ser evidente es que sin una definición de los criterios de evaluación de riesgos, la probabilidad y los puntajes de impacto no son significativos. Qué impactos o probabilidades de '1', '2', '3', '4' o '5' significa, de todos modos? La organización necesitará crear definiciones para su probabilidad e impacto. puntajes para que sean significativos para todas las partes interesadas, y para que proporcionen un Método de evaluación de riesgos.

Definiciones de impacto

Las organizaciones de nivel 2 generalmente se benefician de una mayor participación empresarial en la gestión de la ciberseguridad riesgo que las organizaciones de nivel 1. Debido a esa mayor participación, la evaluación de riesgos Los criterios pueden ser, y deberían ser, más explícitos y detallados que los utilizados por el Nivel 1 organizaciones. Las organizaciones avanzadas pueden considerar más matices en términos de impactos comerciales y tolerancia, y puede emplear objetivos organizacionales con más autoridad.

Una definición de impacto para organizaciones de Nivel 2 puede tener al menos tres tipos de impacto y cinco de impacto puntajes (magnitudes) como la definición representada en la Tabla 35.

Tabla 35 - Definiciones de impacto de ejemplo

Impacto Puntuación	Impacto a la misión	Impactar a Objetivos	Impacto a las obligaciones
	Misión: proporcionar información a ayudar a los pacientes remotos a permanecer saludable.	*Objetivos: operar rentable*	*Obligaciones: los pacientes no deben ser perjudicado por comprometido información.*
1	Los pacientes continúan accediendo información útil, y Los resultados van por buen camino.	Las ganancias están en el objetivo.	Los pacientes no experimentan pérdida de servicio o protección.
2	Algunos pacientes pueden no tener todo la información que necesitan como ellos lo solicitan.	Las ganancias están fuera del objetivo, pero están dentro varianza planificada	Los pacientes pueden estar preocupados, pero no perjudicado
3	Algunos pacientes no pueden acceder la información que necesitan mantener buena salud resultados.	Las ganancias están apagadas varianza planificada y puede tomar un fiscal año para recuperarse.	Algunos pacientes pueden ser perjudicado financieramente o reputacionalmente después compromiso de información o servicios.
4 4	Muchos pacientes constantemente no puede acceder beneficioso información.	Las ganancias pueden tomar más que un fiscal año para recuperarse.	Muchos pacientes pueden ser perjudicado financieramente o reputacionalmente
5 5	Ya no podemos proporcionar información útil para el control remoto pacientes	La organización no puede operar rentable	Algunos pacientes pueden ser perjudicado financieramente, reputacional o fisicamente hasta e incluyendo la muerte.

Antecedentes: definiciones de impacto

Este documento proporciona instrucciones para definir los impactos y los puntajes de impacto (magnitudes) en esta sección con instrucciones más detalladas y ejemplos en las "Técnicas de análisis de riesgos" capítulo. El lector debe comprender antes de continuar que las organizaciones en la mayoría de los casos no debe definir impactos exclusivamente utilizando valores financieros. Si bien el costo es común y consideración casi necesaria al evaluar riesgos y salvaguardas, si es el único criterio, la organización se comunicará con su personal, así como con las partes interesadas y autoridades, ese costo es su única preocupación. El propósito que sirve la organización y el el daño que pueda ocurrir a otros debe ser parte de la evaluación si el riesgo se debe vincular responsablemente con el potencial de daño, y si la evaluación debe ser comprensible para los reguladores y legales autoridades.

Las organizaciones también deberían considerar tener más de tres tipos de impacto en su impacto definiciones si tienen más de una misión, múltiples objetivos y muchas obligaciones que deben tener en cuenta en su análisis de riesgos. Si bien esta expansión puede crear una creciente amplio registro de riesgos, puede ayudar a las organizaciones a sentirse cómodas todos los intereses relevantes fueron considerado en su análisis de riesgos.

Las organizaciones de nivel 2 que anteriormente usaban procesos de análisis de riesgos de nivel 1 pueden aprovechar sus procesos más simples Criterios de evaluación de riesgos que utilizan tres niveles de puntuación de impacto. A los fines de referencia a nuestra organización de ejemplo, un proveedor de información de salud, han pasado por un año o dos de gestión de riesgos y han ganado la atención y la confianza de los gerentes de negocios y ejecutivos Como resultado, su capacidad para evaluar el riesgo de ciberseguridad utilizando criterios comerciales también mejorar.

Podemos ver comparando los criterios de evaluación de riesgos para organizaciones de Nivel 1 en el Capítulo 2 con Tabla 35 que las descripciones detalladas de los impactos han aumentado en dos dimensiones; el número de puntajes de impacto (magnitudes) aumentó de tres a cinco, y hay un tipo de impacto adicional para objetivos comerciales.

Las organizaciones de nivel 2 descubrirán que el uso de un rango de cinco puntajes de impacto (magnitudes) aumenta el utilidad de priorización de riesgos al final de la evaluación de riesgos. Una evaluación de riesgo de tres por tres el modelo de criterios proporciona a las organizaciones seis posibles puntajes de riesgo; 1, 2, 3, 4, 6 y 9. Esto lleva a una agrupación de curso que puede causar riesgos de urgencias algo diferentes indistinguible.

Un modelo de criterios de evaluación de riesgos de cinco por cinco permite 14 posibles puntuaciones de riesgo de; 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 20 y 25. Ahora es probable que se clasifiquen los riesgos de urgencias algo diferentes en diferentes puntajes de riesgo y se distinguirán más fácilmente al priorizarlos.

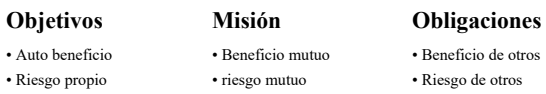
También tenga en cuenta que los puntajes de impacto de '1' y '2' en la Tabla 35 están sombreados en gris para separarlos de las puntuaciones más altas Los puntajes '1' y '2' describen los impactos que generalmente se considerarían como aceptable. El proceso de criterios de aceptación de riesgos se explicará más adelante en el documento, pero es útil considerar ahora que los puntajes '1' y '2' son consistentes en su definición de puntajes de impacto en los tres tipos de impacto, y que las puntuaciones de impacto de '3', '4' o '5' podrían ser consistentemente considerado inaceptablemente alto para los tres tipos de impacto.

El ejemplo de proveedor de información de salud también tiene un nuevo impacto a considerar en la Tabla 35 para ayudar ellos incluyen sus objetivos comerciales en su análisis de riesgos. Los objetivos del negocio son más autocontrolados centrados en misiones y obligaciones, y están alineados con los criterios de éxito comúnmente encontrados en negocio. Algunos ejemplos incluyen rentabilidad, crecimiento, mantenimiento de acreditaciones, clientes satisfacción o retener una posición en el mercado.

Los objetivos se alinean más directamente con lo que comúnmente se considera el "costo" de una salvaguardia. Pero

en lugar de permitir que una organización decida arbitrariamente que una salvaguarda cuesta demasiado, esto
El método de incluir el costo en términos de impactos a los objetivos obliga a la organización a evaluar por qué
Un costo sería excesivo. ¿El costo de la salvaguardia impide los objetivos de rentabilidad? Hace el
salvaguardar la eficiencia o el crecimiento del límite? Esas son ciertamente preocupaciones razonables, siempre que
Los objetivos de rentabilidad están a la par con el impacto de la misión y las obligaciones. *En otras palabras, un
la organización no debería permitir que la rentabilidad sea más importante que dañar a otros o dañar a sus
capacidad para cumplir su misión. Consulte la "Nota sobre el uso de los costos financieros como objetivos" en
Capítulo 5.*

Figura 10 - Objetivos, misión, obligaciones



Las organizaciones están bien atendidas con este modelo porque la gestión empresarial, los técnicos,
El personal de cumplimiento y el asesor legal tienen sus intereses abordados en el análisis de riesgos que
usa estos criterios.

Se proporciona una explicación detallada de cómo desarrollar definiciones de impacto con múltiples ejemplos en
el capítulo "Técnicas de análisis de riesgos".

Definiciones de probabilidad

La definición de probabilidad para una organización de Nivel 2 también debería aumentar en matices a partir de la más simple
Definición de nivel 1, y puede hacerlo agregando dos puntajes más a la tabla como se muestra en la Tabla 36.

Tabla 36 - Definiciones de probabilidad de ejemplo

Probabilidad Puntuación	Previsibilidad
1	**No es previsible** . Esto no es plausible en el medio ambiente.
2	**Previsible** . Esto es plausible, pero no esperado.
3	**Esperado.** Estamos seguros de que esto eventualmente ocurrirá.
4 4	**Común.** Esto sucede repetidamente.
5 5	**Actual** . Esto puede estar sucediendo ahora.

- "No previsible" implica que una amenaza no es plausible en el entorno que se está
  juzgado. La pérdida de medios portátiles puede no ser previsible durante una evaluación de riesgos de un
  aplicación alojada

Página 69

- "Previsible" implica algo plausible, pero la organización sería
  sorprendido si ocurrió. Un ejecutivo fundador que lleva copias de datos confidenciales a
  los competidores pueden considerarse previsibles, incluso si no se espera.
- “Esperado” implica una amenaza que no es común, pero que eventualmente sucedería.
  Se pueden esperar ataques de phishing u otros ataques de ingeniería social en muchos
  ambientes.
- "Común" implica algo que sucede repetidamente, como correos electrónicos mal dirigidos
  con información confidencial, ataques de malware o pérdida de computadoras portátiles y dispositivos móviles.
- "Actual" implica amenazas que rara vez no están presentes, como el escaneo de puertos en el perímetro

dispositivos o compartir información en espacios cuasi públicos como mostradores de farmacia o cajeros de banco.

Cuando los evaluadores de riesgos estiman la probabilidad de una amenaza, seleccionarán los puntajes '1', 2 ',' 3 ',' 4 'o' 5 ' utilizando la definición de previsibilidad como su guía. Las organizaciones pueden agregar límites de tiempo en sus definiciones de previsibilidad (es decir, "previsible dentro de los umbrales de planificación", "esperado dentro del plan quinquenal "o" No previsible en el próximo año fiscal "). Si las organizaciones introducen el tiempo límites en sus definiciones de probabilidad, deben priorizar las inversiones de tratamiento de riesgos para cumplir con estos cronogramas Eso puede ser un desafío excesivo para muchas organizaciones, por lo que deben proceder con cuidado.

Desarrollo de los criterios de evaluación de riesgos.

Debido a que los criterios de evaluación de riesgos están destinados a describir el riesgo tal como se aplica a la organización que posee el riesgo, es apropiado para la alta gerencia que es responsable de misión, objetivos y obligaciones de participar en el desarrollo y aceptación de los criterios.

La Tabla 37 enumera los roles comúnmente involucrados en el desarrollo de criterios de evaluación de riesgos, y el perspectiva interesada que aportan al esfuerzo de definición.

Tabla 37 - Roles involucrados en la definición de los criterios de evaluación de riesgos

Papel	Perspectiva
Director Ejecutivo Director de Operaciones	Asegurar que la misión, los objetivos y las obligaciones del organización están adecuadamente definidos, y para asegurar que un distinción entre impactos aceptables e inaceptables son debidamente delineado.
Director de Cumplimiento	Para asegurar que los intereses de las agencias reguladoras sean debidamente incluido en las definiciones de riesgo.
Director financiero	Para garantizar que los objetivos se definan adecuadamente, particularmente La distinción entre impactos aceptables e inaceptables.
Director de información Jefe de Tecnología	Para garantizar que el rendimiento técnico, el servicio y las capacidades se consideran e incluyen todo tipo de procesos de información más allá de la tecnología
Consejero general Abogado externo	Para garantizar que las obligaciones se definan adecuadamente y que comparar bien con la misión y los objetivos.
Auditoría interna Comité de Auditoría	Asegurar que las inquietudes de las partes interesadas estén bien representado en todas las definiciones de impacto y puntajes.
Clientes / clientes clave Constituyentes clave	Para asegurar que sus intereses estén incluidos en las obligaciones definición.

Ejercicio :

El lector debe desarrollar los criterios de evaluación de riesgos de su organización utilizando los "Criterios: Hoja de trabajo de nivel 2 que se proporciona en el documento complementario *CIS_RAM_Workbook* .

El lector debe considerar:

1. Desarrollar los criterios de evaluación de riesgos en colaboración con gerentes de negocios. y asesoría legal para asegurar que las definiciones de Misión, Objetivos y Obligaciones son sensibles a la organización.
2. Trabajar con un asesor legal para ayudar a garantizar que las definiciones de impacto sean apropiadas abordar los intereses de todas las partes potencialmente afectadas y garantizar ese impacto Las declaraciones parecen equitativas para todas las partes.
3. Consulte la guía para definir y calificar los tipos de impacto en el "Análisis de riesgos Capítulo de Técnicas.

El evaluador de riesgos necesitará usar su juicio profesional para definir los tipos de impacto y describir los niveles de impacto que la organización debe lograr. Porque los criterios de evaluación de riesgos son una declaración de la organización de lo que lograrán en términos de daño a sí mismos y dañar a otros, las organizaciones deben consultar con un asesor legal antes de finalizar estos criterios y tomar decisiones de riesgo basadas en ellos.

Definición de criterios de aceptación de riesgos

Introducción

Debido a que las evaluaciones de riesgo son esencialmente cuestiones de equilibrio, los criterios para aceptar el riesgo debería ayudar a determinar si se logró el equilibrio. En CIS la aceptación del riesgo RAM tiene dos componentes:

- Riesgo apropiado: que la probabilidad de un impacto debe ser aceptable para todos previsiblemente partes afectadas
- Riesgo razonable: que el riesgo planteado por una salvaguarda debe ser menor o igual al riesgo contra el que protege.

Si bien estos componentes se han demostrado brevemente en el Capítulo 1, el "riesgo apropiado" se describirá con más detalle en esta sección. El "riesgo razonable" se describirá más adelante en el Riesgo Sección de recomendaciones de tratamiento más adelante.

Después de establecer las definiciones de impacto y probabilidad, las organizaciones de nivel 2 ahora están bien posicionados para establecer sus criterios de aceptación de riesgos. Recordemos que los impactos se definieron dentro del impacto puntajes que iban de '1' a '5'. Los puntajes de impacto aceptables '1' y '2' se definieron de una manera eso parecería apropiado para las partes interesadas (y está sombreado en gris para indicar su aceptabilidad), y el puntaje de impacto '3' fue el puntaje más bajo inaceptable.

Page 71

Tabla 38 - Impactos inaceptables

Impacto Puntuación	Impacto a la misión	Impactar a Objetivos	Impacto a las obligaciones
	Misión: proporcionar información a ayudar a los pacientes remotos a permanecer saludable.	*Objetivo: operar rentable*	*Obligaciones: los pacientes no deben ser perjudicado por comprometido información.*
1	Los pacientes continúan accediendo información útil, y Los resultados van por buen camino.	Las ganancias están en el objetivo.	Los pacientes no experimentan pérdida de servicio o protección.
2	Algunos pacientes pueden no tener todo la información que necesitan como ellos lo solicitan.	Las ganancias están fuera del objetivo, pero están dentro varianza planificada	Los pacientes pueden estar preocupados, pero no perjudicado
3	Algunos pacientes no pueden acceder la información que necesitan mantener buena salud resultados.	Las ganancias están apagadas varianza planificada y puede tomar un fiscal año para recuperarse.	Algunos pacientes pueden ser perjudicado financieramente o reputacionalmente después compromiso de información o servicios.
4 4	Muchos pacientes constantemente no puede acceder beneficioso información.	Las ganancias pueden tomar más que un fiscal año para recuperarse.	Muchos pacientes pueden ser perjudicado financieramente o reputacionalmente
5 5	Ya no podemos proporcionar información útil para el control remoto pacientes	La organización no puede operar rentable	Algunos pacientes pueden ser perjudicado financieramente, reputacional o fisicamente hasta e incluyendo la muerte.

Y de manera similar, los puntajes de probabilidad estuvieron dentro de un rango de '1' a '5' como se muestra a continuación. Una vez nuestro ejemplo

la organización desarrolla su madurez de gestión de riesgos y está lista para refinar su riesgo distinciones, pueden decidir no tolerar impactos inaceptables si son *previsibles pero no esperado* ('2'), o si se *espera que ocurran* ('3'). Esta sería una decisión mejor tomada por su ejecutivos, y especialmente su equipo de cumplimiento, asesoría general y partes interesadas. Pero en En este caso, el modelo supondrá que seleccionaron un puntaje de probabilidad inaceptable de '3'.

Tabla 39 - Probabilidad inaceptable

Probabilidad Puntuación	Previsibilidad
1	**No es previsible** . Esto no es plausible en el medio ambiente.
2	**Previsible** . Esto es plausible, pero no esperado.
3	**Esperado.** Estamos seguros de que esto eventualmente ocurrirá.
4 4	**Común.** Esto sucede repetidamente.
5 5	**Actual** . Esto puede estar sucediendo ahora.

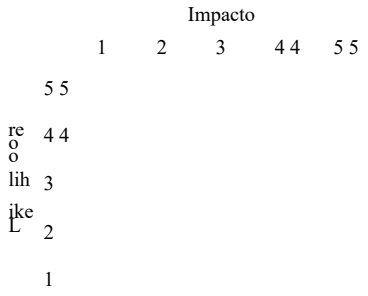
Por lo tanto, las organizaciones de Nivel 2 definirían su aceptación de riesgos de esta manera:

Tabla 40 - Criterios de aceptación del riesgo

Impacto Límite	X	Probabilidad Límite	=	Riesgo Límite
3	X	3	=	9 9
… por lo tanto …				
Riesgo aceptable			<	9 9

En la Figura 11 se muestra un ejemplo del mapa de calor para este criterio de evaluación.
los mapas no se utilizan en CIS RAM, las organizaciones ahora pueden diseñar mapas de calor que representan Aceptabilidad del riesgo basada en los requisitos de la organización y un deber de cuidado con los demás.

Figura 11 - Ejemplo de mapa de calor



Ejercicio :

El lector debe definir los criterios de aceptación de riesgos de su organización utilizando los "Criterios - Nivel Hoja de trabajo de 2 "que se proporciona en el documento complementario *CIS_RAM_Workbook* .

El lector debe considerar:

1. Trabajar con un patrocinador de gestión empresarial que pueda ayudar a garantizar que el riesgo Los criterios de aceptación son sensibles para la organización.
2. Trabajar con un asesor legal para ayudar a garantizar que la definición de aceptación del riesgo aborda los intereses de todas las partes potencialmente afectadas y para garantizar ese impacto Las declaraciones parecen equitativas para todas las partes.

El evaluador de riesgos necesitará usar su juicio profesional para identificar niveles de riesgo aceptables. Debido a que los criterios de aceptación del riesgo son una declaración de la organización de lo que tolerarán en términos de daño a sí mismos y daño a otros, las organizaciones deben consultar con un asesor legal antes de finalizar estos criterios y tomar decisiones de riesgo basadas en ellos.

A medida que las organizaciones evalúan su riesgo utilizando los Controles CIS V7 (modelados en la siguiente sección) podrán determinar automáticamente si el riesgo se evalúa como aceptable o no sin necesidad de considerar la pregunta de manera diferente en cada caso. Una simple estimación de la la probabilidad y el impacto determinarán automáticamente cómo la organización debe priorizar cada riesgo, y si la organización puede aceptar el riesgo de manera segura según corresponda.

Un proceso de evaluación de riesgos basado en activos

Introducción

Las organizaciones de nivel 2 disfrutan de relaciones de colaboración con la gestión no técnica en Gestión de riesgos de seguridad. También tienen el conocimiento y la experiencia para modelar la seguridad de manera plausible amenazas contra los activos de información. En esta sección, la organización de ejemplo se ha vuelto más capaz después de un año de gestión de riesgos y se ha ganado una relación de asociación con departamentos técnicos Han aprendido que los activos de información deben analizarse en función de

su situación y contexto, en lugar de como una sola clase de activos técnicos (un proceso utilizado para Organizaciones de nivel 1 para simplificar sus esfuerzos de evaluación de riesgos).

Como organización de Nivel 2, sus evaluaciones de riesgos primero considerarán los activos de información que son en el alcance de su evaluación. Al considerar esos activos, pensarán a través del CIS Los controles que son apropiados para proteger esos activos, considerarán vulnerabilidades para aquellos controles, y modelarán amenazas previsibles que pueden aprovechar las vulnerabilidades.

Este orden de análisis proporciona un beneficio distintivo a las organizaciones que tienen una mayor madurez. comprensión de los riesgos y salvaguardas de seguridad. Permite a las organizaciones evaluar posibles daños que pueden llegar a activos específicos y a los Controles CIS que deberían protegerlos. Solo entonces lo hace evaluar los riesgos

Las organizaciones que modelan riesgos utilizando CIS Controls V7 pueden encontrar un desafío considerar cómo uno El riesgo está influenciado por otros riesgos relacionados con un activo. Por ejemplo, si un servidor FTP permite terceros los empleados de terceros acceden a él utilizando credenciales compartidas, entonces esos empleados de terceros pueden retener el acceso al servidor FTP después de dejar a su empleador y aumentar el riesgo asociado con CIS Control 16.7 que recomienda un proceso para revocar el acceso al finalizar. Eso podría probablemente aparece como un alto riesgo para la organización. Pero si el evaluador de riesgos también determina que el El servicio FTP solo permite capacidades de escritura (Control CIS 14.7), el riesgo asociado con el Control CIS 16.7 es probable que se reduzca. Evaluaciones de riesgos basadas en el control, como las utilizadas por el Nivel 1 las organizaciones pueden perder esa relación y, como resultado, pueden exagerar el riesgo involucrado en CIS Control 16.3.

Además del análisis de riesgos que toma este orden ligeramente diferente en su modelado de amenazas, Nivel 2 Las organizaciones también estimarán el riesgo con criterios de riesgo más complejos. Por su relación Con la gestión empresarial, las organizaciones de nivel 2 recibirán cierta presión de las empresas gerentes para refinar su priorización de riesgos, y evaluar el riesgo utilizando más explícitamente Criterios de impacto basados.

Esta sección describirá y trabajará a través de la evaluación de riesgos de una organización de Nivel 2 utilizando el CIS Controles, y mostrará cómo evaluar los riesgos utilizando los criterios de evaluación de riesgos que son apropiado para organizaciones de nivel 2.

Esta sección del documento describirá un registro de riesgos que está disponible como plantilla en el documento complementario *CIS_RAM_Workbook* .

El registro de riesgos

A medida que la organización de Nivel 2 prepare su evaluación de riesgos, reunirán su lista de activos de información y alinearlos con los controles CIS que son apropiados para proteger a aquellos activos de información. Esta sección demostrará este proceso utilizando la plantilla de registro de riesgos proporcionado en el documento complementario *CIS_RAM_Workbook* para organizaciones de Nivel 2.

El mapa de diseño de un registro de riesgos para una organización de Nivel 2 se muestra en la Figura 12.

Page 74

Figura 12 - Mapa de diseño del registro de riesgos

El registro de riesgos para organizaciones de Nivel 2 es una lista de riesgos identificados y sus riesgos recomendados. tratamientos, también conocidos como "salvaguardas". Cada fila representa un riesgo y el riesgo que lo acompaña. recomendación de tratamiento Las partes del registro de riesgos son:

A. Los encabezados de columna y el texto guía ayudan al lector o al evaluador de riesgos a comprender el información contenida en la columna.
B. Los activos de información identifican los elementos y procesos que se están analizando.
C. Los controles CIS ayudan al evaluador de riesgos a considerar los controles que deberían estar en su lugar para Proteger los activos de información.
D. El "modelo de amenaza" incluye los siguientes elementos:
    a. Una descripción de cómo se implementa el control CIS en el entorno.
    si. La vulnerabilidad que puede existir si el control no se implementa completamente.
    do. La amenaza que puede comprometer el activo debido a la vulnerabilidad.
E. La evaluación de riesgos estima la probabilidad de que la amenaza tenga éxito, y el impactos a la misión, objetivos y obligaciones si lo hiciera. La evaluación incluye el puntaje de riesgo resultante, calculado como un producto de la probabilidad y el más alto de los tres puntajes de impacto.
F. Los tratamientos de riesgo se recomiendan para los riesgos que se evalúan como inaceptablemente altos. Se describen las salvaguardas que se basan en los controles CIS, y a su vez son evaluado por el riesgo que pueden representar para la misión y los objetivos. Un "riesgo de salvaguardia" Se calcula la puntuación que debe ser inferior a los criterios de aceptación del riesgo, y el riesgo que se pretende abordar

El proceso

El evaluador de riesgos de nivel 2 analizará los riesgos utilizando un enfoque basado en activos, comenzando el evaluación considerando los activos de información que pretenden proteger. Porque esto el proceso creará invariablemente más detalles en el registro de riesgos (en forma de múltiples filas en el registro de riesgo para cada activo y cada control de CIS aplicable) las organizaciones pueden desear comenzar su

análisis de riesgo utilizando el método basado en control de Nivel 1. Este método primero analiza cómo el CIS Los controles se aplican generalmente al medio ambiente. El evaluador de riesgos de nivel 2 puede examinar el activos de información que están protegidos de manera diferente a la práctica estándar en una fila separada.

Página 75

El proceso de evaluación de riesgos basado en activos se ilustra en la Figura 13.

Figura 13: Proceso de análisis de riesgos para organizaciones de nivel 2

El proceso de evaluación de riesgos basado en activos para las organizaciones de Nivel 2 está destinado a garantizar que cada El activo de información está protegido por los Controles CIS de manera apropiada para su riesgo particular.
Este análisis basado en activos se realiza siguiendo los pasos que se detallan a continuación:

1. Seleccione los activos de información o las clases de activos que se enumeran en el inventario de activos. Grabar los activos seleccionados en la celda "Activo de información" en esa fila.
    a. Si la organización de Nivel 2 ya ha completado un registro de riesgos que evaluó todos de los Controles CIS, ya que se aplican generalmente a la organización, luego el El análisis de riesgos puede comenzar seleccionando los activos que figuran en el registro de riesgos.
    si. Las organizaciones pueden desear evaluar las clases de activos en lugar de los activos individuales para la eficiencia Como ejemplo, a menudo hay un conjunto de tecnologías similares que están idénticamente configurados y gestionados. En tales circunstancias, enumere estos como las clases de activos son apropiadas porque cada uno de estos elementos será similar al conjunto. Elementos únicos como un enrutador central, un equilibrador de carga, una sola instancia de un aplicación, o un sistema operativo único debe analizarse por sí solo.
2. Modele las amenazas utilizando el siguiente enfoque:
    a. Considere cada activo de información o clase de activo uno por uno.
    si. Empareje cada activo de información o clase de activo con los controles CIS que están apropiado para protegerlos. Esto se ve ayudado por la categorización de "Tipo de activo" de Controles CIS V7. Por ejemplo, escritorios de usuario, servidores de aplicaciones, multifunción Las impresoras y tabletas son sistemas que se pueden combinar con los controles CIS que se clasifican para "Sistemas".
    do. Agregue una fila al registro de riesgos para cada emparejamiento de un Control CIS y el activo de información o clase de activo.
    re. Nota: Es probable que sea demasiado lento evaluar todos los emparejamientos adecuados entre activos de información y controles CIS aplicables. Si bien ese análisis sería óptimo, es más apropiado para las organizaciones priorizar el emparejamiento de información activos y clases de activos con los cinco principales controles CIS y otros controles que puede ser de interés para la organización. La gestión de riesgos es un ciclo continuo. eso permitirá a las organizaciones abordar más riesgos con el tiempo a medida que su seguridad programa madura.
3. Reúna evidencia de qué tan bien cada activo está protegido por su Control CIS emparejado.
    a. La evidencia puede ser en forma de entrevistas, una revisión de configuraciones, un prueba de vulnerabilidad, una prueba de penetración, una evaluación de un sistema o dispositivo usando Políticas de SCAP, o una revisión de evidencia como registros y registros.
4. Describa cómo se aplica el control al activo de información o clase de activo en el "Actual Control "celda de esa fila.

5. Considere la diferencia entre el control CIS y el control actual y determine
si existe una deficiencia en cómo se implementa y opera el control actualmente. Si el
el control actual no se implementa como se describe, ¿cómo se describiría esto como un
¿vulnerabilidad?
    a. Considere el objetivo del control CIS. Por ejemplo, CIS Control 10.3 afirma
    "Pruebe la integridad de los datos en los medios de copia de seguridad de forma regular mediante la realización de datos
    proceso de restauración para garantizar que la copia de seguridad funcione correctamente ". Su objetivo es
    para garantizar que los datos de respaldo en los medios de almacenamiento se puedan recuperar cuando sea necesario. Si
    el control actual no cumple el objetivo, luego indique la brecha como
    vulnerabilidad en la celda de vulnerabilidad, como: "No estamos seguros de que nuestro
    los datos de respaldo se pueden recuperar de los medios de respaldo ".
6. Ahora considere la amenaza que podría ocurrir debido a la vulnerabilidad.
    a. La vulnerabilidad anterior podría combinarse con la amenaza: "Las fallas del sistema pueden
    resultar en una recuperación de datos tan antigua como un mes, o puede requerir entrada manual
    de documentos en papel ".
7. Luego, calcule la probabilidad de que la amenaza tenga éxito y el impacto que puede crear.
    a. La estimación de probabilidad puede ser un desafío al principio, pero los criterios de evaluación de riesgos
    proporcionar alguna orientación en ese proceso de estimación. También se proporciona orientación en
    el capítulo "Técnicas de análisis de riesgos".
    si. Los puntajes de impacto deben proporcionar estimaciones del impacto que tal amenaza causaría
    crear. Considere las puntuaciones de probabilidad e impacto como un par. En otras palabras,
    "¿Cuál es la probabilidad de que resulte este impacto?"
    Proporcionar más orientación.
8. La puntuación de riesgo se calculará automáticamente multiplicando la puntuación de probabilidad por
El más alto de los tres puntajes de impacto.

Nivel 2 Evaluación de riesgos Ejemplo 1 - Caso de negocio basado en riesgos
Mientras realiza su evaluación de riesgos, la organización de Nivel 2 se encuentra con un común
pregunta con la que tratan las organizaciones; ¿Cuándo una razón comercial justifica excepciones a la seguridad?
políticas? Esta pregunta surge cuando consideran el Control CIS 15.9 que dice: "Desactivar la conexión inalámbrica
acceso periférico de dispositivos (como Bluetooth y NFC), a menos que dicho acceso sea necesario para
propósito de negocio."

Las organizaciones comúnmente aceptan riesgos que vienen con excepciones de política, y lo hacen al
documentando esa aceptación del riesgo. Pero si toman estas decisiones sin cuidado, coherente
análisis en consideración de los impactos previsibles para ellos mismos y otros, luego su riesgo
La aceptación en sí misma es arriesgada.

En el caso de CIS Control 15.9, la organización utiliza sistemas accesibles por Bluetooth en regiones
clínicas para apoyar a sus pacientes. Los pacientes llevan "dispositivos diarios" electrónicos que monitorean su salud
estado y almacenar datos de salud como diarios. Bluetooth se utiliza en clínicas para conectar el dispositivo diario
controladores a los dispositivos de diario para leerlos para diagnósticos, para recibir datos de los dispositivos y
para transmitir firmware actualizado a esos dispositivos. Esto es indudablemente digno de un documento documentado.
necesidad de Negocios. ¿Pero sigue siendo irrazonablemente riesgoso hacerlo?

Uso de la plantilla de registro de riesgos para organizaciones de Nivel 2 que se proporciona en el documento
CIS_RAM_Workbook , la organización primero enumera el activo de información que está evaluando.

Tabla 41 - Ejemplo de activo de información

Activo de información
Controladores de dispositivo de diario

Luego se encuentran con el Control CIS que plantea la pregunta sobre el riesgo aceptable para las empresas.

Tabla 42 - Ejemplo de control CIS

CEI Controlar	Descripción
15,9	Desactive el acceso periférico inalámbrico de dispositivos (como Bluetooth y NFC), a menos que dicho acceso sea necesario para un fin comercial.

El evaluador de riesgos debe pensar y registrar el modelo de amenaza para este riesgo. Recordemos que el el modelo de amenaza considera su control actual, qué vulnerabilidades resultantes pueden existir y qué Las amenazas serían motivo de preocupación para ellos. Mientras que los controladores del dispositivo diario deben emparejarse con el diario dispositivos, la organización se da cuenta de que sus controladores de dispositivos de diario habilitados para Bluetooth y el los atacantes pueden acceder a los archivos ubicados en ellos utilizando métodos de ataque fácilmente disponibles.

Entonces las siguientes tres columnas del registro de riesgos se verían así:

Tabla 43 - Ejemplo de modelo de amenaza

Controlar	Vulnerabilidad	Amenaza
Cada dispositivo de diario es unido al diario controlador de dispositivo usando una sola vez, seis dígitos código que se muestra en el controlador y ingresado en el dispositivo. En este punto, todos los archivos transferencias y firmware actualizaciones entre Los dispositivos están habilitados.	Los controladores de dispositivo de diario están utilizando una versión obsoleta de Bluetooth para soportar dispositivos diarios más antiguos Los dispositivos Bluetooth pueden manipular Servicios de Bluetooth en el diario controladores de dispositivos para obtener acceso a archivos y comandos en el controladores	Los hackers pueden caminar clínicas con Bluetooth dispositivos que están preparados para hackear el dispositivo diario controladores que usan ataques como Blueborne y puede acceder a cientos de archivos de datos del paciente, también como firmware

Pero este puede no ser el único riesgo que se puede considerar en este escenario. Otro riesgo plausible podría ser que el pirata informático pudiera poner firmware comprometido en los controladores del dispositivo diario para permitir ellos para controlar los dispositivos después de las actualizaciones de firmware. Los ataques de denegación de servicio también pueden ocurrir. Los ataques de Man-in-the-Middle también son posibles. Los evaluadores de riesgos pueden estar preocupados de que un interminable se podrían crear varios modelos de amenazas para cualquier emparejamiento entre activos de información y CIS Controles, haciendo que el ejercicio de evaluación de riesgos sea interminable. Por supuesto, el evaluador de riesgos debe limitar la cantidad de teorización que hacen al modelar amenazas, centrándose principalmente en la mayoría combinaciones de amenazas plausibles dado el entorno de seguridad. *Como organización de nivel 2, deben confiar en personal capacitado y recursos que los ayudan a enfocarse en las amenazas más plausibles para sus medio ambiente* .

El modelo de amenaza ahora está claramente establecido y hace posible que la organización pueda estimar probabilidad e impacto del escenario. Recordemos las definiciones de los puntajes de impacto y probabilidad que creó la organización de nivel 2. Los puntajes de impacto se actualizan en la Tabla 44.

78 de 1189.

Tabla 44 - Definiciones de impacto de ejemplo

Impacto Puntuación	Impacto a la misión	Impactar a Objetivos	Impacto a las obligaciones
	Misión: proporcionar información a ayudar a los pacientes remotos a permanecer saludable.	*Objetivo: operar rentable*	*Obligaciones: los pacientes no deben ser perjudicado por comprometido información.*
1	Los pacientes continúan accediendo	Las ganancias están en el objetivo. Los pacientes no experimentan	

	información útil, y Los resultados van por buen camino.		pérdida de servicio o protección.
2	Algunos pacientes pueden no tener todo la información que necesitan como ellos lo solicitan.	Las ganancias están fuera del objetivo, pero están dentro varianza planificada	Los pacientes pueden estar preocupados, pero no perjudicado
3	Algunos pacientes no pueden acceder la información que necesitan mantener buena salud resultados.	Las ganancias están apagadas varianza planificada y puede tomar un fiscal año para recuperarse.	Algunos pacientes pueden ser perjudicado financieramente o reputacionalmente después compromiso de información o servicios.
4 4	Muchos pacientes constantemente no puede acceder beneficioso información.	Las ganancias pueden tomar más que un fiscal año para recuperarse.	Muchos pacientes pueden ser perjudicado financieramente o reputacionalmente
5 5	Ya no podemos proporcionar información útil para el control remoto pacientes	La organización no puede operar rentable	Algunos pacientes pueden ser perjudicado financieramente, reputacional o fisicamente hasta e incluyendo la muerte.

Recuerde también que las definiciones de impacto para las organizaciones de Nivel 2 incluyen criterios para la organización objetivos porque esas organizaciones generalmente se benefician de la colaboración con las empresas gestión que invierte en el éxito del programa de seguridad de la información. Estas Los gerentes a menudo traen a la discusión los objetivos estratégicos y tácticos de la organización para el éxito. Pero también tenga en cuenta que esta definición de impacto contiene cinco magnitudes de impacto. Cinco puntajes de impacto ayudar a las organizaciones de Nivel 2 a refinar sus estimaciones de impacto en términos más tangibles que las tablas con tres niveles de puntaje y ayudarlos a refinar su puntaje de riesgo para distinguir mejor entre los riesgos de Prioridad variable. Los puntajes de impacto aceptables de '1' y '2' están sombreados para diferenciarlos de los más altos, puntajes de impacto inaceptables.

Las probabilidades se definieron de manera similar con cinco puntajes potenciales por razones similares, como se muestra en la Tabla 45

Tabla 45 - Ejemplos de definiciones de probabilidad

Probabilidad Puntuación	Previsibilidad
1	**No es previsible** . Esto no es plausible en el medio ambiente.
2	**Previsible** . Esto es plausible, pero no esperado.
3	**Esperado.** Estamos seguros de que esto eventualmente ocurrirá.
4 4	**Común.** Esto sucede repetidamente.
5 5	**Actual** . Esto puede estar sucediendo ahora.

La organización cree que el modelo de amenaza que documentaron anteriormente, que los piratas informáticos podrían piratear los controladores de dispositivos diarios utilizando algo similar a un ataque Blueborne, es previsible, y tal vez se espera que ocurra. Si bien el escenario probablemente no sería esperado para la mayoría organizaciones, nuestra organización de ejemplo opera en entornos donde competidores y

Página 79

los estados adversarios tienen un interés activo en comprometer sus sistemas y han demostrado su capacidad en el pasado. Entonces deciden que su puntaje de probabilidad para este riesgo será '3'.

En ese escenario, también esperan que su misión se vea afectada hasta el punto en que algunos (no muchos) pacientes perderían su capacidad de obtener un dispositivo diario que funcione y, por lo tanto, No acceder a la información que necesitan para mantener buenos resultados de salud. Ellos seleccionan una misión impacto de '3'.

Tal ocurrencia haría que la organización reinvierta masivamente e inmediatamente en su infraestructura clínica; una inversión que no están preparados para hacer ahora y que podría tomar más de un año para recuperarse. Eso crearía un impacto de objetivos de '4'.

Y finalmente, creen que cada controlador de dispositivo diario contendría no más de 100 pacientes registros en cualquier momento, dadas sus rutinas de trabajo y horarios de servicio. La información del paciente podría usarse para dañar a los pacientes de manera reputacional si los hackers supieran cómo rastrear las identificaciones de los pacientes registrar las condiciones de salud de cada paciente y luego actuar de manera maliciosa con esa información. Esto es no es un impacto plausible, por lo que seleccionan un impacto de obligaciones de '2'.

Un riesgo que se espera que ocurra (probabilidad = 3) de una manera que impide que algunos pacientes Acceso a la información (impacto de la misión = 3), que tomaría más de un año recuperarse de financieramente (impacto de objetivos = 4), y eso puede causar preocupación pero no dañar a los pacientes (impacto de las obligaciones = 2) aparecería como tal en la Tabla 46.

Tabla 46 - Ejemplo de estimación de riesgo

Amenaza Probabilidad	Misión Impacto	Objetivos Impacto	Obligaciones Impacto	Puntuación de riesgo
3	3	4 4	2	12

El puntaje de riesgo es el producto del puntaje de probabilidad y el más alto de los tres puntajes de impacto, que en este caso es '3 x 4 = 12'.

Recuerde también que los criterios de aceptación de riesgos para la organización de Nivel 2 se ven así:

Tabla 47 - Criterios de aceptación del riesgo

Impacto Límite	X	Probabilidad Límite	=	Riesgo Límite
3	X	3	=	9 9
… por lo tanto …				
Riesgo aceptable			<	9 9

Un riesgo aceptable sería aquel que se evalúe a cualquier valor por debajo de '9'. Pero el riesgo de cómo el la organización protege sus controladores de dispositivos diarios utilizando su implementación de CIS Control 15.9 es '12' y es inaceptablemente alto.

Este análisis de riesgos se muestra en la Tabla 48 en una sola tabla para reunir todos estos elementos. juntos. Para fines de visualización de documentos, este análisis de riesgo se muestra en formato vertical en lugar de que horizontal como aparecería en un registro de riesgos. Los ejemplos que se describen en este La sección está contenida en el libro de trabajo *CIS_RAM_Workbook* .

Tabla 48 - Ejemplo de análisis de riesgos para dispositivos protegidos por el control CIS 15.9

Análisis de riesgo	Valor
Activo de información	Controladores de dispositivo de diario
Control CIS	15,9
Descripción	Deshabilite el acceso periférico inalámbrico de dispositivos (como Bluetooth y NFC), a menos que dicho acceso sea necesario para un fin comercial.
Controlar	Cada dispositivo de diario se une al controlador del dispositivo de diario mediante un código único de seis dígitos que se muestra en el controlador y ingresado en el dispositivo. En este punto, todas las transferencias de archivos y firmware Las actualizaciones entre dispositivos están habilitadas.
Vulnerabilidad	Los controladores de dispositivo de diario utilizan una versión obsoleta de Bluetooth para admitir dispositivos de agenda más antiguos. Los dispositivos Bluetooth pueden manipular los servicios de Bluetooth en los controladores del dispositivo diario para obtener acceso a archivos y comandos en los controladores.
Amenaza	Los hackers pueden recorrer clínicas con dispositivos Bluetooth que son preparado para hackear controladores de dispositivos diarios mediante ataques como Blueborne, y también puede acceder a cientos de archivos de datos de pacientes como firmware
Probabilidad de amenaza	3

Impacto de la misión	3
Objetivos Impacto	4 4
Obligaciones Impacto	2
Puntuación de riesgo	**12**
Aceptabilidad del riesgo	**Inaceptable**

Entonces, si bien existe una necesidad comercial documentada de que estos dispositivos operen servicios Bluetooth, el riesgo de hacerlo con este dispositivo sigue siendo inapropiadamente alto (ya que los criterios de aceptación de riesgo son menos de '9' y el puntaje de riesgo observado es '12'). La organización querrá abordar esto con un salvaguarda del tratamiento de riesgo, que se demostrará en las Recomendaciones de tratamiento de riesgo sección más adelante en este capítulo.

Sin embargo, debido a que el proceso de evaluación de riesgos para las organizaciones de Nivel 2 comienza en el activo, lo hacemos tener otras oportunidades para considerar cómo otros controles pueden proteger el activo de una manera que puede reducir el riesgo que acabamos de observar.

Podemos examinar cómo este proceso proporciona a la organización de Nivel 2 una visión más profunda del riesgo con Los siguientes dos ejemplos.

Nivel 2 Evaluación de riesgos Ejemplo 2 - Reducción de riesgos a través de controles relacionados
La organización de Nivel 2 está considerando riesgos para sus activos de información al vincular el activo con CIS Controles apropiados para protegerlo. CIS Controls V7 ayuda en este emparejamiento al proporcionar un esquema de clasificación para los controles llamado "Tipo de activo". Si un controlador de dispositivo diario es un sistema que tiene conectividad de red, entonces el evaluador de riesgos de la organización de Nivel 2 puede mirar a través de los Controles CIS que están asociados con las familias "Sistema" y "Red" para identificar otros controles que serían apropiados para proteger a los controladores.

Página 81

Ya han evaluado que CIS Control 15.9 no protege el diario conectado por Bluetooth controladores de dispositivos lo suficientemente bien. Pero no están sin alternativas. La organización piensa a través de otros controles que usan para proteger sus dispositivos de agenda y encontrar el Control CIS 16.3 que dice: "Requerir autenticación multifactor para todas las cuentas de usuario, en todos los sistemas, ya sea administrado en el sitio o por un proveedor externo ".

Esto es interesante para ellos, porque los dispositivos de diario usan "tokens blandos" en forma de certificados que están destinados a rastrear los dispositivos de diario para fines de inventario. Pero los certificados son muy robusto, y están vinculados a los privilegios de acceso a archivos en los controladores de dispositivos. Podría esto la implementación de CIS Control 16.3 representa un riesgo aceptable para los controladores de dispositivos diarios, y ¿Podrían reducir el riesgo citado para CIS Control 15.9?

El evaluador de riesgos de la organización de nivel 2 prueba esta idea en la Tabla 49. Observe cómo está ahora el control se describe utilizando más detalles que el primer intento de analizar este riesgo.

Tabla 49 - Ejemplo de análisis de riesgos para dispositivos protegidos por el control CIS 16.3

Análisis de riesgo	Valor
Activo de información	Controladores de dispositivo de diario
Control CIS	16,3
Descripción	Requerir autenticación multifactor para todas las cuentas de usuario, en todos sistemas, ya sea administrados en el sitio o por un proveedor externo.
Controlar	Mientras que los dispositivos de diario pueden conectarse a los controladores de dispositivos de diario a través de Bluetooth usando un código único de seis dígitos, acceso a archivos existentes con la información del paciente en el controlador se otorga utilizando el certificado suave único en cada dispositivo diario.
Vulnerabilidad	Se pueden adivinar los códigos de seis dígitos o se pueden robar certificados blandos de dispositivos de diario y almacenados en sistemas atacantes.
Amenaza	Los hackers deben robar certificados blandos de los dispositivos de diario, luego adivinar uno:

	códigos de tiempo de seis dígitos para acceder a los archivos del paciente en el dispositivo diario controladores
Probabilidad de amenaza	1
Impacto de la misión	3
Objetivos Impacto	4 4
Obligaciones Impacto	2
Puntuación de riesgo	**4 4**
Aceptabilidad del riesgo	**Aceptable**

Dado este método para la autenticación de dos factores, el modelo de amenaza para los piratas informáticos que adquieren pacientes los registros de los controladores de dispositivos diarios ya no son previsibles utilizando el modelo de amenaza que el Nivel 2 organización evaluada. Y si ese es el caso del control de autenticación de dos factores, entonces También debe influir en el riesgo asociado con el Control CIS 15.9 que se evaluó anteriormente. Entonces el el evaluador de riesgos vuelve a evaluar ese riesgo nuevamente mientras hace referencia a los controles identificados para el Control CIS 16.3 para ver si entienden el riesgo de manera diferente. Nuevamente, tenga en cuenta que el evaluador de riesgos describió el control con más detalle que el primer intento, y agregó una condición a la amenaza contra CIS Control 16.3.

Page 82

Tabla 50 - Ejemplo de análisis de riesgo revisado para dispositivos protegidos por el control CIS 15.9

Análisis de riesgo	Valor
Activo de información	Controladores de dispositivo de diario
Control CIS	15,9
Descripción	Deshabilite el acceso periférico inalámbrico de dispositivos (como Bluetooth y NFC), a menos que dicho acceso sea necesario para un fin comercial.
Controlar	[Complementado por CIS Control 16.3] Cada dispositivo diario está unido a el controlador del dispositivo de diario utilizando un código de seis dígitos de una sola vez que es aparece en el controlador y se ingresa en el dispositivo. En este punto, Todas las transferencias de archivos y actualizaciones de firmware están habilitadas. Sin embargo, los archivos solo pueden acceder dispositivos que utilicen certificados de software que sean asociado con privilegios de acceso en controladores de dispositivos diarios.
Vulnerabilidad	Los controladores de dispositivo de diario utilizan una versión obsoleta de Bluetooth para admitir dispositivos de agenda más antiguos. Dispositivos Bluetooth con los certificados blandos incautados pueden manipular los servicios de Bluetooth en el diario controladores de dispositivos para obtener acceso a archivos y comandos en el controladores
Amenaza	Los hackers pueden recorrer clínicas con dispositivos Bluetooth que son preparado con certificados blandos específicos del dispositivo para hackear el dispositivo diario controladores que usan ataques como Blueborne. Los hackers deben robar certificados blandos de dispositivos de diario, luego adivine códigos únicos de seis dígitos para acceder a los archivos de pacientes en los controladores de dispositivos diarios.
Probabilidad de amenaza	1
Impacto de la misión	3
Objetivos Impacto	4 4
Obligaciones Impacto	2
Puntuación de riesgo	**4 4**
Aceptabilidad del riesgo	**Aceptable**

Como se esperaba, el riesgo asociado con CIS Control 15.9 se reduce debido a la probabilidad de que El modelo de amenaza se reduce cuando se tiene en cuenta la inverosimilitud de los hackers que acceden a archivos en Los controladores del dispositivo diario. De hecho, la probabilidad del escenario de amenaza es tan baja que el riesgo es

aceptable.
El enfoque basado en activos para el análisis de riesgos presenta claramente una ventaja para las organizaciones al Proporcionar una imagen más completa y realista del riesgo real de que una información
El activo está expuesto a.

Nivel 2 Evaluación de riesgos Ejemplo 3 - Nuevas perspectivas del riesgo
No todos los análisis de riesgo basados en activos reducirán las estimaciones de riesgo, por supuesto. Algunos resaltarán riesgos que las organizaciones rara vez consideran. En este ejemplo, la organización de nivel 2 emparejó los controles CIS para las defensas de malware con los controladores de dispositivos diarios y se dieron cuenta de que tenían un problema. CEI Control 8.1 dice: "Utilice software antimalware administrado centralmente para monitorear y defender cada una de las estaciones de trabajo y servidores de la organización ".

Page 83

Pero el proveedor del controlador del dispositivo diario no admite ni proporciona una aplicación antivirus para su sistema operativo: una distribución Linux personalizada. Mientras que los controladores del dispositivo diario son Sistemas "sin cabeza", tienen aplicaciones de administración web que proporcionan funciones administrativas para operadores de controlador, y se pueden administrar a través de sesiones de terminal a través de puertos de consola. los la organización no quiere violar su acuerdo de soporte con el proveedor compilando y ejecutando una aplicación antivirus en los controladores.

Al ejecutar un análisis de riesgos, la organización determinará si el riesgo de malware es alto suficiente para requerir un software antivirus. Su hallazgo se ilustra en la Tabla 51.

Tabla 51 - Ejemplo de análisis de riesgos para dispositivos protegidos por CIS Control 8.1

Análisis de riesgo	Valor
Activo de información	Controladores de dispositivo de diario
Control CIS	8.1
Descripción	Utilice software antimalware administrado centralmente para continuamente supervisar y defender cada una de las estaciones de trabajo de la organización y servidores
Controlar	El software antimalware no está permitido en el dispositivo diario controladores
Vulnerabilidad	Las vulnerabilidades son limitadas porque los vectores comunes para recibir malware como clientes de correo electrónico y navegadores web no están instalados en los controladores. Los atacantes tendrían que descargar malware ejecutables desde Internet usando scripts o comandos bash. La línea de comando, por diseño, solo es accesible desde la terminal conexiones al puerto de la consola. Los ataques de Bluetooth aún pueden permitir que se ejecuten ejecutables de malware cargado en un espacio de archivos asociado con una cuenta anónima. La aplicación de administración web en cada controlador se ha probado como vulnerable a la ejecución de código arbitrario, secuencias de comandos entre sitios y otros ataques
Amenaza	Los hackers pueden implantar malware en controladores de dispositivos diarios a través de Uso indebido de Bluetooth y aproveche la aplicación de administración web vulnerabilidades para ejecutar archivos o iniciar scripts.
Probabilidad de amenaza	3
Impacto de la misión	3
Objetivos Impacto	4 4
Obligaciones Impacto	3
Puntuación de riesgo	**12**
Aceptabilidad del riesgo	**Inaceptable**

Esto parece más serio para la organización de lo que hubieran pensado originalmente. Todavía preocupada por los ataques que han visto en el pasado, la organización se da cuenta de que es muy probable que que sean atacados a través de una vulnerabilidad de aplicación web como lo sería a través de un Bluetooth vulnerabilidad. Implantar un virus utilizable a través de un exploit de Bluetooth o una carga arbitraria de archivos

requiere un hacker con paciencia y habilidad, por lo que la puntuación de probabilidad de '3' para "Esperado" parece más adecuado que un '4' para "Común".

Los desafíos que enfrenta la organización son múltiples en este riesgo: no pueden instalar un antivirus aplicación, ni una aplicación web más segura en los controladores de dispositivos de diario, pero el riesgo de El malware es claramente demasiado alto. Evaluarán posibles salvaguardas mientras desarrollan su riesgo recomendaciones de tratamiento en el siguiente paso de su proceso de evaluación de riesgos más adelante en este capítulo.

Ejercicio :

El lector debe consultar la plantilla Registro de riesgos - Nivel 2 que se proporciona en el documento complementario *CIS_RAM_Workbook.* Pueden usar la plantilla de registro de riesgos para ingrese un conjunto de riesgos asociados con los Controles CIS y los activos de información que están en Alcance de su evaluación.

Al hacer este ejercicio, el lector debe considerar:

1. Asegurar que todos los activos de información dentro del alcance o clases de activos sean evaluados.
2. No "hirviendo el océano". No todos los activos se pueden evaluar prácticamente contra todos Controles CIS aplicables en una sola evaluación. Priorizar los controles que protegen activos de información que parecen vulnerables o que protegen sistemas de alto valor y información.
3. Considere evaluar todos los activos contra los primeros cinco controles CIS para abordar la mayoría Causas comunes de incidentes de ciberseguridad.
4. Si un control o activo de información requiere un examen para comprender su valor real configuración y efectividad.
5. Si la organización puede tolerar la cantidad de esfuerzo y tiempo que el riesgo evaluación requiere.
    a. La organización debe usar análisis de alto nivel (revisión de políticas y entrevistas) si no tienen mucho tiempo y recursos.
    si. Los activos de información deben ser probados y examinados con más detalle a medida que pasa el tiempo. permite.
    do. La organización debe planificar evaluaciones de riesgos recurrentes para identificar más riesgos. a través del tiempo.
6. Colaborar con expertos en temas de seguridad de la información para ayudar a modelar amenazas que son previsibles en el medio ambiente, y para ayudar a evaluar la efectividad de salvaguardas actuales.

El evaluador de riesgos deberá usar su criterio profesional para seleccionar los controles y activos de información y modelar amenazas que deben analizarse en la evaluación de riesgos. Los expertos en seguridad de la información pueden necesitar ser incluidos en el proceso para asegurar que el riesgo El análisis se realiza adecuadamente.

Resumen de evaluación de riesgos de nivel 2

Después de haber analizado un conjunto de riesgos contra un único activo de información, la organización de Nivel 2 se da cuenta de las ventajas de obtener una visión más completa de sus riesgos:

1. Cuando las organizaciones consideran los impactos a sus objetivos, los evaluadores de riesgos incluyen negocios intereses en su análisis de riesgos, involucrando así a colaboradores no técnicos en la decisión de riesgos fabricación.

2. Cuando las organizaciones agregan puntajes de impacto (magnitudes) y puntajes de probabilidad, pueden hacer distinciones más refinadas entre riesgos y puede priorizarlos de manera más razonable.
3. El emparejamiento de activos de información con múltiples controles CIS proporciona una información más completa y quizás una comprensión precisa del riesgo real para esos activos.
4. El emparejamiento de activos de información con múltiples controles CIS también incita a los evaluadores de riesgos a considerar las amenazas que de otro modo habrían descuidado.

Recomendaciones de tratamiento de riesgos

Introducción

Las organizaciones a menudo piensan en las salvaguardas de seguridad como obstáculos para los negocios y la productividad. Las salvaguardas a menudo hacen que el personal tome medidas adicionales para acceder a los sistemas o la información, o para obtener la aprobación de las actividades comerciales normales. Las salvaguardas requieren inversiones en tiempo y dinero, que compiten con otras prioridades. Y si se vuelven demasiado perjudiciales para la organización misión y objetivos, las salvaguardas de seguridad pueden ser desagradables y evitadas.

De hecho, las salvaguardias disruptivas a menudo hacen que el personal trabaje a su alrededor solo para obtener su trabajo hecho, lo que crea más riesgo.

Pero las recomendaciones de tratamiento de riesgo pueden y deben dar como resultado salvaguardas que sean demostrables razonable. Y mientras obtener una definición clara de "salvaguardas razonables" ha sido un desafío en las comunidades legales, regulatorias y de seguridad de la información, el CIS RAM proporciona un Solución práctica. Los evaluadores de riesgos evalúan las recomendaciones de tratamiento de riesgos para determinar si una salvaguarda de seguridad es razonable por; comparar la salvaguardia con el riesgo que se pretende reducir, y al comparar la salvaguarda con los criterios de aceptación del riesgo.

Las recomendaciones de tratamiento de riesgos son simples de evaluar una vez que los criterios de evaluación de riesgos y Se ha establecido un análisis de riesgo inicial. El proceso se realiza en los siguientes pasos:

1. Mientras examina un riesgo inaceptablemente alto, revise el Control CIS que corresponde con el riesgo y recomendar una forma factible para que la organización implemente o mejore ese controlar.
2. Si ese control no es factible en el corto plazo, recomiende otros controles CIS relacionados con El riesgo que se puede utilizar para reducirlo.
3. Evaluar el riesgo de la salvaguarda recomendada para comprender la carga que representaría a la organización. Luego compare ese riesgo de salvaguarda con los criterios de aceptación de riesgo para determinar si es apropiado
4. Compare también el riesgo evaluado de la salvaguarda recomendada con el riesgo observado para determinar si la salvaguarda es razonable (salvaguardas con puntajes de riesgo más bajos que los riesgos observados son razonables)
5. Clasifique los riesgos por su puntaje de riesgo para priorizar los riesgos y los tratamientos de riesgo que el la organización invertirá en

Esta sección muestra estos pasos en detalle al describir el proceso y luego al modelar el riesgo tratamientos para los riesgos inaceptablemente altos que se evaluaron en secciones anteriores.

El lector debe revisar las definiciones de 'razonable' y 'apropiado' que se proporcionan en el glosario. Estos términos se usarán regularmente en esta sección y tienen significados distintos.

1. Apropiado: una condición en la cual los riesgos para los activos de información no previsiblemente crearán daño que es mayor que la organización o sus constituyentes pueden tolerar.
2. Razonable: una condición en la cual las salvaguardas no crearán una carga para la organización eso es mayor que el riesgo contra el cual está destinado a proteger.

Objetivos de tratamiento de riesgos
El objetivo de las recomendaciones de tratamiento de riesgos bien formadas es crear una lista priorizada de salvaguardas de seguridad de la información que proporcionarían protecciones apropiadas mientras no posan demasiado Una gran carga para el propósito de la organización.

Los ejercicios de recomendación de tratamiento de riesgo que se demuestran en esta sección examinan el riesgos inaceptables que se ilustraron anteriormente en el documento y seleccionarán los Controles CIS que reduciría esos riesgos en un grado que sea razonable (no excesivamente pesado) y apropiado (no inaceptablemente dañino).

Recomendaciones de salvaguardas de tratamiento de riesgos de los controles CIS V7
A medida que examinamos riesgos inaceptablemente altos, recomendaremos salvaguardas basadas en CIS Controles. Pero algunas de las garantías que una organización está preparada para implementar y operar es posible que no se implemente exactamente como se describe en CIS Controls V7. Este proceso toma en cuenta cómo seleccionar controles que aborden los riesgos y cómo determinar si son diseñado de una manera que tenga sentido en el contexto tanto del riesgo como de la carga potencial para el organización.

Recuerde la relación entre los riesgos analizados y sus tratamientos de riesgo recomendados en la Figura 14)

Figura 14 - Balance dentro del análisis de riesgo central

Un riesgo y su salvaguarda propuesta se evalúan utilizando el mismo criterio. Si un propuesto la salvaguarda tiene un riesgo más alto (su "riesgo de salvaguarda") que los criterios de aceptación del riesgo, entonces no es apropiado. Si la salvaguardia tiene una puntuación más alta que el riesgo observado, entonces no es razonable.

Los ejercicios en esta sección se centrarán en hacer coincidir los análisis de riesgo completados (en azul) con los nuevos garantías recomendadas (en verde).

Ejemplo de tratamiento de riesgos 1 - Control CIS 8.1
El ejercicio que demostró el análisis de riesgos en la Tabla 51 mostró a la organización de Nivel 2 que su El riesgo de malware en sus controladores de dispositivos diarios (CIS Control 8.1) era demasiado alto. La organización no se le permitió agregar software antimalware a los controladores del dispositivo.

Para recomendar salvaguardas basadas en controles alternativos, el evaluador de riesgos revisa CIS Control 8.1 para entender su objetivo. CIS Control 8.1 tiene la intención de que todos los dispositivos deberían activamente buscar malware y actividad de intrusión, bloquear la actividad e informarla a la administración de seguridad sistemas.

La organización enfrenta un desafío cuando se da cuenta de que el proveedor del controlador del dispositivo diario no admite protección contra malware en los controladores, y la organización puede violar el términos de servicio del contrato del proveedor si instalan protección contra malware disponible.

Hasta que el fabricante del controlador del dispositivo distribuya una distribución más segura de su producto, la organización deberá considerar algunas salvaguardas para proteger el dispositivo diario vulnerable controladores La administración de TI recomendó que la organización simplemente instale protección contra malware

en los controladores y arriesgarse con el vendedor. Pero antes de comprometerse con este plan, ellos trabajó con el evaluador de riesgos para analizar el riesgo de hacerlo. La Tabla 52 ilustra su análisis.

Nota: El evaluador de riesgos registrará cómo abordarán su riesgo al indicar "Aceptar" “Reducir”, “Transferir” o “Evitar”. *Aceptar* y *reducir* riesgos será intuitivo para el lector. Un la organización puede *transferir* un riesgo mediante la contratación de un tercero que puede manejar el riesgo mejor, o mediante

adquirir una póliza de seguro contra el riesgo. La organización también puede *evitar* el riesgo por no participar más tiempo en los procesos o manejar los activos de información que causan el riesgo

Tabla 52 - Ejemplo de recomendación de tratamiento de riesgos para el control CIS 8.1

Análisis de riesgo	Valor
Control CIS	8.1
Descripción	Utilice software antimalware administrado centralmente para supervisar y defender continuamente cada una de las organizaciones estaciones de trabajo y servidores.
Activo de información	Controladores de dispositivos diarios.
Controlar	El software antimalware no está permitido en el dispositivo diario controladores
Vulnerabilidad	Las vulnerabilidades son limitadas porque los vectores comunes para recibir malware como clientes de correo electrónico y navegadores web no están instalados en los controladores. Los atacantes necesitarían descargar ejecutables de malware de Internet usando scripts o comandos bash. La línea de comando, por diseño, solo es accesible desde la terminal conexiones al puerto de la consola. Los ataques de Bluetooth aún pueden permitir que los ejecutables de malware ser cargado en un espacio de archivos asociado con un anónimo cuenta. La aplicación de administración web en cada controlador tiene sido probado como vulnerable a la ejecución de código arbitrario, secuencias de comandos entre sitios y otros ataques.
Amenaza	Los hackers pueden implantar malware en controladores de dispositivos diarios a través del uso indebido de Bluetooth y aprovechar la web vulnerabilidades de la aplicación de administrador para ejecutar archivos o iniciar guiones.
Probabilidad de amenaza	3
Impacto de la misión	3
Objetivos Impacto	4 4
Obligaciones Impacto	3
Puntuación de riesgo	**12**
Aceptabilidad del riesgo	**Inaceptable**
Opción de tratamiento de riesgo	Reducir
Salvaguardia recomendada	Instale la aplicación antimalware y la intrusión basada en host agentes de prevención en controladores de dispositivos diarios.

Page 88

Análisis de riesgo	Valor
Salvaguardar el riesgo	Malware identificado con firma y RAM volátil común las vulnerabilidades serán detectadas, prevenidas e informadas al Consola de gestión central. Si el proveedor ve el malware y los agentes IPS en los controladores durante sus sesiones de servicio trimestrales, pueden cancelar esos contratos de servicio, retrasando el servicio en sistemas defectuosos hasta que se puedan instalar nuevas imágenes en los dispositivos.
Salvaguardia Amenaza Probabilidad 4	
Salvaguardar el impacto de la misión	3

Objetivos de salvaguarda Impacto	3
Obligaciones de salvaguardia Impacto	2
Puntuación de riesgo de salvaguarda	**12**
Aceptabilidad del riesgo	**Inaceptable**

La organización ha evaluado la recomendación de la administración de instalar el antimalware los agentes son tan riesgosos como el riesgo observado que están tratando de abordar. El estimado salvaguardar el riesgo es igual al riesgo observado, pero en base a la preocupación de la organización de que el se esperaba que el proveedor forzara la nueva imagen en los controladores del dispositivo diario, lo que significaba que esperaban comprometer su misión y objetivos.

El evaluador de riesgos ahora puede aconsejar a la gerencia que no instale el software de seguridad directamente, pero luego debe proporcionar alternativas.

Page 89

Antecedentes: ¿qué tan realistas son las estimaciones de riesgo de salvaguarda?

Los lectores críticos se preguntarán cómo la organización y su asesor de riesgos sabrán si Sus estimaciones de riesgo de salvaguardia son realistas. Después de todo, ¿cómo pueden saber prospectivamente qué su riesgo estaría en tal situación?

Hay dos elementos importantes a tener en cuenta al obtener comodidad con esta práctica; Comprender las expectativas legales y regulatorias para la gestión de riesgos, y la información estándares de seguridad para evaluar las salvaguardas después de que se hayan implementado.

Ley y regulación: las leyes y regulaciones generalmente esperan que el análisis de riesgos evalúe salvaguardas que se requieren para lograr el cumplimiento, y se espera que el análisis de riesgos sea realizado por personas debidamente capacitadas e informadas. Estos análisis no garantizan seguridad que es suficiente contra cualquier amenaza, pero proporcionan un plan para mejorar seguridad y cumplimiento que se prioriza por la probabilidad de daño, y que no tiene intolerable daño como su objetivo.

Normas de gestión de riesgos de seguridad de la información: evaluación de riesgos de seguridad de la información Los estándares en los que se basa la RAM CIS operan dentro de programas de gestión de riesgos más completos y ciclos ISO 27005 opera dentro de la familia de estándares ISO 27000, y NIST 800-30 funciona dentro de las publicaciones especiales del NIST. Cada una de estas familias de estándares requiere continua análisis de salvaguardas de seguridad, incluido el análisis de controles después de que se hayan implementado para determinar si son efectivos para abordar sus objetivos de seguridad. Recomendado

por lo tanto, las salvaguardas deben evaluarse nuevamente después de la implementación para asegurarse de que lograr sus objetivos previstos.

Ejemplo de tratamiento de riesgos 2 - Control CIS 8.1
A medida que la organización considere un tratamiento de riesgo alternativo, recurrirán a otros controles CIS para ver qué alternativas están disponibles para ellos.

CIS proporciona al público un documento titulado *Modelo de ataque comunitario de CIS.* [18] El documento enumera todos los controles CIS y los asocia con el papel que desempeñan en cada etapa del incidente preparación y respuesta; planificación, detección y defensa. Mediante el uso de la comunidad CIS Modelo de ataque, una organización puede encontrar controles CIS relacionados y alternativos que pueden sustituir a controles que no pueden implementar lo suficiente.

Al revisar el Modelo de ataque comunitario (Figura 15), el evaluador de riesgos puede identificar rápidamente qué controles deben considerar si CIS Control 8.1 no es factible.

El modelo de ataque comunitario se proporciona en el *CIS_RAM_Workbook* en una pestaña titulada "Ruta de ataque Modelos "para la conveniencia del lector, y se pueden descargar en el sitio web de CIS.

Una instantánea parcial del marco demuestra lo que el evaluador de riesgos de Nivel 2 encontró a medida que buscó controles alternativos.

[18] Se puede acceder al *Modelo de ataque comunitario* aquí: https://www.cisecurity.org/white-papeles / modelo de ataque comunitario cis /

Página 90

Figura 15 - Modelo de ataque parcial a la comunidad

Los evaluadores de riesgos pueden hacer referencia al Modelo de ataque comunitario para encontrar controles que puedan ser complementarios y alternativos a las salvaguardas recomendadas que están evaluando. Si una la organización lucha por implementar un subcontrol, podrían buscar controles que jueguen de manera similar papel en el Modelo de ataque comunitario para encontrar controles alternativos que puedan ayudarlos a cumplir con el

mismo objetivo de seguridad. Por ejemplo, si una organización no puede usar fácilmente los registros de auditoría para *detectar entrega* de un tipo de amenaza, pueden buscar otro control en la celda que se cruza con el *detectar la* fila y la columna de *entrega* para encontrar controles similares, y eventualmente ver la red controles de detección de intrusos, que pueden ser más útiles en su entorno.

Dados los objetivos de CIS Control 8.1 para proteger sistemas contra malware e identificables intrusiones, el evaluador de riesgos revisa el Modelo de ataque comunitario y encuentra anti-malware en las células esa dirección que *protege* contra la *entrega* , y para *proteger* y *detectar la inicial compromiso* . Detectar la entrega de malware parece ser un buen lugar para comenzar sus defensas ya que está más cerca de la amenaza que están abordando en su análisis de riesgos, por lo que revisan los Controles CIS que están en la celda en la intersección de *Detectar* y *Entrega* para considerar las opciones.

Los sistemas de detección de intrusiones de red y los sistemas de prevención de intrusiones de red ("IDS / IPS") son interesante para la organización como protección de la capa de red. El evaluador de riesgos revisa el sub controles dentro de CIS Control 12 "Defensa de límites" para ver cómo se describe IDS. Control CIS 12.6 "Implementar el sensor IDS basado en red" presenta una opción atractiva para ellos porque su actual El uso de los controladores del dispositivo diario durante las visitas clínicas se realiza dentro de las LAN inalámbricas móviles que propio y de control. Un IDS ligero sería una opción plausible en ese caso.

Pero un IDS / IPS ligero en esas LAN inalámbricas portátiles reduciría su malware y riesgo de intrusión en sus controladores de dispositivos diarios? Modelan CIS Control 12.6 como salvaguarda contra este mismo riesgo para ver si sería razonable.

Page 91

Tabla 53 - Ejemplo de recomendación de tratamiento de riesgos para CIS Control 8.1 utilizando CIS Control 12.6

Análisis de riesgo	Valor
Control CIS	8.1
Descripción	Utilice software antimalware administrado centralmente para supervisar y defender continuamente cada una de las organizaciones estaciones de trabajo y servidores.
Activo de información	Controladores de dispositivos diarios.
Controlar	El software antimalware no está permitido en el dispositivo diario controladores
Vulnerabilidad	Las vulnerabilidades son limitadas porque los vectores comunes para recibir malware como clientes de correo electrónico y navegadores web no están instalados en los controladores. Los atacantes necesitarían descargar ejecutables de malware de Internet usando scripts o comandos bash. La línea de comando, por diseño, solo es accesible desde la terminal conexiones al puerto de la consola. Los ataques de Bluetooth aún pueden permitir que los ejecutables de malware ser cargado en un espacio de archivos asociado con un anónimo cuenta. La aplicación de administración web en cada controlador tiene sido probado como vulnerable a la ejecución de código arbitrario, secuencias de comandos entre sitios y otros ataques.
Amenaza	Los hackers pueden implantar malware en controladores de dispositivos diarios a través del uso indebido de Bluetooth y aprovechar la web vulnerabilidades de la aplicación de administrador para ejecutar archivos o iniciar guiones.
Probabilidad de amenaza	3
Impacto de la misión	3
Objetivos Impacto	4 4
Obligaciones Impacto	3
Puntuación de riesgo	**12**

Aceptabilidad del riesgo	**Inaceptable**
Opción de tratamiento de riesgo	Reducir
Salvaguardia recomendada	[CIS Control 12.6] Agregue un dispositivo IDS / IPS liviano a Las LAN portátiles que operan en visitas clínicas eran diarios Se utilizan controladores de dispositivos.
Salvaguardar el riesgo	Los dispositivos IDS / IPS detectarán ataques reconocibles de otros hosts dentro de la LAN que intentan entregar e implementar malware para controladores. IDS / IPS puede no detectar la carga útil de malware de hosts que conectarse a controladores a través de protocolos encriptados.
Salvaguardia Amenaza Probabilidad 2	

Página 92

Análisis de riesgo	Valor
Salvaguardar el impacto de la misión	3
Objetivos de salvaguarda Impacto	3
Obligaciones de salvaguardia Impacto	2
Puntuación de riesgo de salvaguarda	**6 6**
Aceptabilidad del riesgo	**Aceptable**

Aunque CIS Control 12.6 no presenta una solución antimalware directa, este escenario sí presentar un riesgo aceptable y un riesgo razonable. El tratamiento de riesgo recomendado reduce el probabilidad de un ataque exitoso en los controladores de dispositivos diarios sin eliminarlo en este caso.

La gerencia está convencida de que la salvaguarda recomendada es apropiada, pero eso también interesado en otra opción presentada por CIS Control 12.11 para utilizar la autenticación de dos factores para inicie sesión en las sesiones de terminal en los controladores de dispositivos diarios. Si la autenticación de dos factores proporciona riesgo aún menor, y el proveedor del controlador del dispositivo diario admite la opción, entonces esto puede ser un mejor protección que el IDS / IPS ligero.

Recuerde que los dispositivos de agenda ya almacenan certificados blandos cifrados para ayudar a autenticar los dispositivos para sus cuentas en los controladores. Al consultar con el proveedor, la organización ve que La opción cert está disponible para sistemas de administrador que también se conectan a los controladores. Cuando el los administradores del sitio de la organización se conectan a los controladores de dispositivos diarios mientras están en el sitio, ellos acceder a sesiones de terminal utilizando SSH, el único protocolo disponible para ellos. Múltiples certificados suaves pueden se utilizará tanto para autenticar las sesiones SSH como para ejecutar comandos en los controladores.

Modelan este tratamiento de riesgo alternativo a continuación.

Tabla 54 - Ejemplo de recomendación de tratamiento de riesgos para el Control CIS 8.1 utilizando el Control CIS 12.11

Análisis de riesgo	Valor
Control CIS	8.1
Descripción	Utilice software antimalware administrado centralmente para supervisar y defender continuamente cada una de las organizaciones estaciones de trabajo y servidores.
Activo de información	Controladores de dispositivos diarios.
Controlar	El software antimalware no está permitido en el dispositivo diario controladores
Vulnerabilidad	Las vulnerabilidades son limitadas porque los vectores comunes para recibir malware como clientes de correo electrónico y navegadores web no están instalados en los controladores. Los atacantes necesitarían descargar ejecutables de malware de Internet usando

scripts o comandos bash.

La línea de comando, por diseño, solo es accesible desde la terminal conexiones al puerto de la consola.

Los ataques de Bluetooth aún pueden permitir que los ejecutables de malware ser cargado en un espacio de archivos asociado con un anónimo cuenta. La aplicación de administración web en cada controlador tiene

Página 93

Análisis de riesgo	Valor
	sido probado como vulnerable a la ejecución de código arbitrario, secuencias de comandos entre sitios y otros ataques.
Amenaza	Los hackers pueden implantar malware en controladores de dispositivos diarios a través de exploits de aplicaciones web mientras operan en entornos clínicos
Probabilidad de amenaza	3
Impacto de la misión	3
Objetivos Impacto	4 4
Obligaciones Impacto	3
Puntuación de riesgo	**12**
Aceptabilidad del riesgo	**Inaceptable**
Opción de tratamiento de riesgo	Reducir
Salvaguardia recomendada	[Control CIS 12.11] Requerir todo el uso de SSH y todo Autenticación en controladores de dispositivos de diario para usar certificados blandos almacenado en dispositivos cliente como un segundo factor de autenticación.
Salvaguardar el riesgo	Todos los intentos de acceder a los servicios SSH en el dispositivo diario los controladores serán bloqueados a menos que los clientes usen certificados blandos para acceder a sesiones SSH. Los atacantes pueden aprovechar y reutilizar certificados blandos durante visitas clínicas de 8 horas de duración y pueden atacar controladores como resultado.
Salvaguardia Amenaza Probabilidad 1	
Salvaguardar el impacto de la misión	3
Objetivos de salvaguarda Impacto	3
Obligaciones de salvaguardia Impacto	2
Puntuación de riesgo de salvaguarda	**3**
Aceptabilidad del riesgo	**Aceptable**

Parece que el riesgo de salvaguarda obtenido al usar el Control CIS 12.11 es mucho menor que el salvaguardar el riesgo modelado por la opción de usar CIS Control 12.6. Y porque el vendedor ya admite autenticación de múltiples factores, la solución casi ya está configurada. La organización elige usar el Control 12.11 de CIS como su control de tratamiento de riesgo para proteger su dispositivo diario controladores contra malware hasta que el proveedor proporcione una solución más sólida.

Page 94

Ejercicio :

El lector debe usar la plantilla Registro de riesgos - Nivel 2 que se proporciona en el documento complementario *CIS_RAM_Workbook* para ingresar recomendaciones de tratamiento de riesgo para cada riesgo evaluado como inaceptablemente alto.

El lector debe considerar:

1. Si se puede mejorar una salvaguarda existente y cómo se haría.
2. Si una salvaguarda basada en un Control CIS diferente proporcionaría riesgo apropiado
3. Colaborar con expertos en temas de seguridad de la información para ayudar a modelar eficacia potencial de las salvaguardas recomendadas.

El evaluador de riesgos necesitará usar su juicio profesional para diseñar y recomendar salvaguardas de seguridad de la información y evaluar prospectivamente el riesgo que pueden presentar. Los expertos en seguridad de la información pueden necesitar ser incluidos en el proceso para asegurar que el riesgo El análisis se realiza adecuadamente.

Resumen de recomendaciones de tratamiento de riesgos

Las recomendaciones de tratamiento de riesgos son una parte crítica de las evaluaciones de riesgos para asegurarse de que La organización ha desarrollado un plan para abordar los riesgos sin crear otros riesgos para el organización o sus constituyentes. Algunos de los beneficios que se han demostrado sobre esto proceso son:

1. Las organizaciones pueden demostrar a los gerentes de negocios colaboradores cómo se recomienda se pueden implementar salvaguardas de seguridad sin crear demasiada carga para el Misión empresarial y objetivos.
2. Las organizaciones pueden demostrar a los reguladores y otras autoridades legales que las salvaguardas son razonables porque el riesgo de salvaguarda de la salvaguardia (la "carga" para el organización) no es mayor que el riesgo que se pretende reducir.
3. Las organizaciones pueden demostrar que las salvaguardas recomendadas serían apropiadas mostrando que previsiblemente no crearían un impacto que sería intolerable para el organización o sus constituyentes.
4. Las organizaciones pueden encontrar valioso evaluar múltiples salvaguardas en caso de que una salvaguarda es más razonable (crea un riesgo aún menor) que otra salvaguarda.
5. Los evaluadores de riesgos descubrirán que sus colegas comprenderán y apreciarán los riesgos y controla cuándo los evaluadores de riesgos y los expertos en la materia colaboran en la evaluación de riesgos, y planificación de salvaguardas.

El proceso para evaluar riesgos y recomendar tratamientos de riesgo apropiados ha sido demostrado a nivel general. Sin embargo, algunas preguntas probablemente permanezcan para el lector evaluar salvaguardas, estimar probabilidad y la idoneidad de modelos de probabilidad en riesgo análisis. Estos temas más detallados se analizarán en el capítulo "Técnicas de análisis de riesgos".

Page 95

Capítulo 4: Evaluación de riesgos basada en amenazas Instrucciones para organizaciones de niveles 3 y 4

Las instrucciones de evaluación de riesgos de los **niveles 3 y 4** son adecuadas para las organizaciones que se ajustan al perfil de organizaciones de Nivel 3 y Nivel 4 según lo descrito por el Marco de Ciberseguridad NIST **.** Estas Las organizaciones pueden identificarse con las siguientes características:

- **NIST Tier** : organizaciones de niveles 3 y 4. Los materiales de los niveles 3 y 4 son los más adecuados para organizaciones que utilizan criterios basados en el riesgo para políticas de toda la empresa y procesos.
- **Experiencia** : la organización tiene recursos y capacidades para analizar amenazas de seguridad, y planificar salvaguardas apropiadas para el riesgo, incluidas las habilidades disponibles para modelar cómo las amenazas operaría dentro de su organización.
- **Tiempo** : la organización puede invertir tiempo para analizar los riesgos a nivel específico. sistemas, dispositivos y aplicaciones en el contexto de amenazas específicas.

Este capítulo consta de secciones que abordan cada una de las actividades específicas dentro de un riesgo. evaluación. Los lectores deben participar en este capítulo leyendo primero el texto en cada sección, y luego realizar los ejercicios que se recomiendan para cada sección. El material presentado en la RAM CIS es sustancialmente diferente de muchos otros estándares y modelos de evaluación de riesgos, así que el lector primero debe comprender el objetivo de cada sección y luego practicar lo que aprende utilizando plantillas que se proporcionan en el documento complementario *CIS_RAM_Workbook* .

Al realizar su primera evaluación de riesgos basada en RAM CIS, las organizaciones deben tener cuidado de no trate de "hervir el océano". Los organismos reguladores y las normas de seguridad de la información entienden por igual que no todos los riesgos pueden identificarse en una sola evaluación. Las organizaciones deben continuamente y Evaluar regularmente los riesgos para identificar, comprender y gestionar los riesgos a lo largo del tiempo.

El proyecto de evaluación de riesgos

Visión general

Las evaluaciones de riesgos son proyectos con pasos claros para preparar, conducir y reportar riesgos análisis. Y aunque los proyectos de evaluación de riesgos se pueden modelar con un plan de proyecto, cada El enfoque del proyecto de la organización variará dependiendo de factores como la disponibilidad de recursos y se desarrollará con el tiempo a medida que las organizaciones se vuelvan más capaces en su madurez de ciberseguridad. Esta La sección describirá un proyecto básico de evaluación de riesgos, sus componentes y variaciones, y presente orientación para preparar el plan del proyecto.

Cómo y cuándo usar el análisis de riesgos basado en amenazas

El análisis de riesgos basado en amenazas que se describe en este capítulo requiere un esfuerzo considerablemente mayor. y experiencia que los métodos de análisis utilizados por las organizaciones de Nivel 1 y Nivel 2. Esto es principalmente debido a un paso de análisis - modelado de ruta de ataque - que precede a la evaluación de riesgos.

El modelado de la ruta de ataque proporciona a las organizaciones información valiosa sobre los riesgos de seguridad de la información analizando cómo responderían sus activos de información a los escenarios de ataque conocidos.

Por ejemplo, si una organización quiere comprender su susceptibilidad a un troyano que se extrae datos de una base de datos específica, trazarían escenarios plausibles de cómo un troyano ingresar a su entorno, se instalaría en una estación de trabajo, obtendría privilegios para base de datos, accedería a los datos de la base de datos y luego enviaría los datos robados a un objetivo sistema. El modelo de ruta de ataque identifica estos pasos y enumera los activos de información que

ser incluido en ese ataque. Esto da como resultado una lista de activos de información y amenazas que comprometerlos. Los evaluadores de riesgos luego basarían su análisis de riesgos en esa lista de activos y amenazas

Este capítulo demostrará cómo el análisis de riesgos basado en amenazas ofrece información útil sobre la información. riesgos de seguridad, pero el lector puede entender cómo una evaluación integral de riesgos utilizando este enfoque podría llevar mucho tiempo.

Las organizaciones que comienzan a practicar análisis de riesgos basados en amenazas pueden querer responder preguntas de riesgo específicas, en lugar de planificar una evaluación de riesgos completa basada en su exhaustiva análisis. Algunos ejemplos de usos pueden ser:

1. Después de haber completado una evaluación de riesgos utilizando el enfoque descrito para el Nivel 2 organizaciones, el evaluador de riesgos puede querer entender qué tan bien preparada la información los activos son para prevenir amenazas específicas y actuales.
2. La precisión del puntaje de riesgo de un activo específico se cuestiona porque el personal Creemos que el activo está bien protegido por capas de seguridad.
3. La exhaustividad de una evaluación de riesgo reciente es cuestionable porque está interesado las partes creen que algunas vulnerabilidades de los activos no fueron bien pensadas.
4. Mientras planifica la remediación del riesgo, la gerencia se pregunta si resolver el riesgo para uno El activo de información tendrá un efecto en cascada y beneficioso sobre un conjunto de otros activos.

Para estos escenarios y otros similares, el análisis de riesgos basado en amenazas puede ayudar a las organizaciones evaluar el riesgo dentro del contexto de una cadena de eventos sin tener que aplicar un escrutinio tan profundo para cada activo en el alcance de la evaluación de riesgos.

Evaluación de riesgos Gestión de proyectos Esquema del proyecto
Las evaluaciones de riesgos son proyectos que requieren planificación, identificación de activos y propietarios de activos, programación de sesiones y recopilación de datos. CIS RAM proporciona instrucciones detalladas para estos pasos de gestión y planificación de proyectos en los capítulos para organizaciones de Nivel 1 y Nivel 2 que puede beneficiarse de estas instrucciones tácticas.

Dada la madurez esperada de las organizaciones Tier 3 y Tier 4, estas instrucciones no se proporcionará en este capítulo. Sin embargo, el lector puede beneficiarse de revisar esos materiales en esos capítulos antes de continuar con el Capítulo 4.

El documento complementario *CIS_RAM_Workbook* proporciona plantillas para la programación de proyectos. y el alcance de las organizaciones Tier 3 y Tier 4, si es necesario.

Definición de criterios de evaluación de riesgos

Introducción

Los criterios de evaluación de riesgos son las declaraciones numéricas y en lenguaje sencillo que una organización utiliza para evaluar su riesgo de ciberseguridad. La forma más familiar de cálculos de riesgo, "Riesgo = Probabilidad x Impacto "es la base para el análisis de riesgos en la RAM CIS. Pero es solo el punto de partida para el análisis de riesgos.

Los criterios de evaluación de riesgos deben ser significativos para las organizaciones que los utilizan, por lo que deben ser vinculado al beneficio y daño potencial que la organización puede crear. El impacto de un La violación de la seguridad cibernética puede dañar a la organización misma, puede dañar la capacidad de la organización para cumplir con éxito su misión, o puede dañar a otros.

Debido a que las fallas de ciberseguridad impactan a las partes dentro y fuera de una organización, el riesgo Los criterios de evaluación deben ser universalmente significativos y deben abordar los intereses de todos partes potencialmente afectadas. Además, los criterios de evaluación de riesgos deben demostrar a las autoridades,

tales como reguladores y litigantes, que la organización considera el riesgo de daño a otros como tanto como el riesgo de daño a sí mismos.

Si bien estos requisitos pueden parecer complejos, el método presentado en esta sección Abordarlos suficientemente utilizando una técnica que sea fácil de desarrollar y usar.

Criterios de evaluación de riesgos Fundamentos
El análisis de riesgos proporcionado en el CIS RAM es, en su raíz, una cuestión de equilibrio entre el potencial de daños futuros contra la cierta carga de una salvaguardia. Los reguladores y litigantes tienen durante mucho tiempo consideró este equilibrio como clave para actuar como una "persona razonable". La estructura central de un La declaración de riesgo se proporciona a continuación para ilustrar el concepto central de equilibrio.

Figura 16 - Balance dentro del análisis de riesgo central

Observe algunas cosas de inmediato con el modelo de análisis de riesgos en la Figura 16.

- Si bien las organizaciones generalmente evalúan el riesgo observado para determinar si deberían abordarlo o aceptarlo, esta declaración de riesgo compara deliberadamente el riesgo observado con un salvaguarda propuesta.
- El criterio que evalúa el riesgo también evalúa la salvaguarda.
- El impacto del riesgo estima el potencial de daño para la organización y el daño potencial contra otros.

Los evaluadores de riesgos comparan los riesgos con sus salvaguardas propuestas para determinar si las salvaguardas crearían un riesgo previsiblemente menor que el estado actual. Para lograr esto, el el evaluador evalúa el riesgo estatal actual (o "riesgo observado") y la salvaguarda propuesta utilizando Los mismos criterios para garantizar la comparabilidad.

Esta comparación evita que las organizaciones implementen salvaguardas excesivamente pesado, o que crea nuevos riesgos inaceptables. Por ejemplo, una organización que usa software que ya no es compatible con el proveedor, pero depende de ese software para negocios críticos propósitos, deben encontrar métodos alternativos para identificar y controlar posibles riesgos de seguridad hasta que reemplacen el software. Si la gerencia recomienda cambiar rápidamente a inferior, pero software seguro, la organización puede sufrir un mayor impacto en su misión que la seguridad riesgo que están tratando de evitar.

Al considerar CIS Control 18: Seguridad del software de aplicación, una declaración de riesgo puede estimar la previsibilidad de una amenaza impactante. El riesgo puede establecerse tal como aparece en la Tabla 55 (donde la puntuación de riesgo '12' es un producto de la probabilidad '3' y la puntuación de impacto más alta '4'):

Tabla 55 - Ejemplo de declaración de riesgo central

Riesgo observado	Impacto de probabilidad de	Nosotros	Impactar a Otros	Riesgo Puntuación
Los hackers pueden explotar a los no compatibles, Pero aplicación crítica.	3	3	4 4	**12**

Un evaluador de riesgos debería recomendar y evaluar una salvaguarda para reducir la alta seguridad riesgo, como se ilustra en la Tabla 56. Aquí, la organización se daría cuenta de que la probabilidad de un El impacto negativo para su misión es mayor que el riesgo estatal actual. Este es un caso obvio de la carga es mayor que el riesgo y una salvaguarda recomendada no es razonable.

Tabla 56 - Ejemplo de salvaguarda propuesta irrazonable

Propuesto Salvaguardia	Nuevo riesgo	Probabilidad	Impactar a Nosotros	Impactar a Otros	Salvaguardia Riesgo

Reemplazar aplicación con inferior, Aplicación segura.	La solicitud será funcionar ineficientemente	5 5	3	1	**15**

Cuando se enfrenta a este análisis, la organización debe encontrar otra forma de abordar el riesgo. Este proceso se describirá más adelante en este capítulo en la sección Tratamiento de riesgos Recomendaciones

Pero lo que debería ser evidente es que sin una definición de los criterios de evaluación de riesgos, la probabilidad y los puntajes de impacto no son significativos. Qué impactos o probabilidades de '1', '2', '3', '4' o '5' significa, de todos modos? La organización necesitará crear definiciones para su probabilidad e impacto. puntajes para que sean significativos para todas las partes interesadas, y para que proporcionen un Método de evaluación de riesgos.

Definiciones de impacto

Las organizaciones de Nivel 3 y Nivel 4 generalmente se benefician de una mayor participación empresarial en la gestión riesgo de ciberseguridad que las organizaciones de Nivel 1. Debido a esa mayor participación, el riesgo Los criterios de evaluación pueden ser, y deberían ser, más explícitos y detallados que los utilizados por Tier 1 organizaciones. Las organizaciones avanzadas pueden considerar más matices en términos de impactos comerciales y tolerancia, y puede emplear objetivos organizacionales con más autoridad.

Una definición de impacto para las organizaciones de Nivel 3 y Nivel 4 puede parecerse a la que se muestra en la Tabla 57.

Tabla 57 - Definiciones de impacto de ejemplo

Impacto Puntuación	Impacto a la misión	Impactar a Objetivos	Impacto a las obligaciones
	Misión: proporcionar información a ayudar a los pacientes remotos a permanecer saludable.	*Objetivos: operar rentable*	*Obligaciones: los pacientes no deben ser perjudicado por comprometido información.*
1	Los pacientes continúan accediendo información útil, y Los resultados van por buen camino.	Las ganancias están en el objetivo.	Los pacientes no experimentan pérdida de servicio o protección.
2	Algunos pacientes pueden no tener todo la información que necesitan como ellos lo solicitan.	Las ganancias están fuera del objetivo, pero están dentro varianza planificada	Los pacientes pueden estar preocupados, pero no perjudicado
3	Algunos pacientes no pueden acceder la información que necesitan mantener buena salud resultados.	Las ganancias están apagadas varianza planificada y puede tomar un fiscal año para recuperarse.	Algunos pacientes pueden ser perjudicado financieramente o reputacionalmente después compromiso de información o servicios.
4 4	Muchos pacientes constantemente no puede acceder beneficioso información.	Las ganancias pueden tomar más que un fiscal año para recuperarse.	Muchos pacientes pueden ser perjudicado financieramente o reputacionalmente
5 5	Ya no podemos proporcionar información útil para el control remoto pacientes	La organización no puede operar rentable	Algunos pacientes pueden ser perjudicado financieramente, reputacional o fisicamente hasta e incluyendo la muerte.

Antecedentes: definiciones de impacto

Este documento proporciona instrucciones para definir los impactos y los puntajes de impacto (magnitudes) en

esta sección con instrucciones más detalladas y ejemplos en las "Técnicas de análisis de riesgos" capítulo. El lector debe comprender antes de continuar que las organizaciones en la mayoría de los casos no debe definir impactos exclusivamente utilizando valores financieros. Si bien el costo es común y consideración casi necesaria al evaluar riesgos y salvaguardas, si es el único criterio, la organización se comunicará con su personal, así como con las partes interesadas y autoridades, ese costo es su única preocupación. El propósito que sirve la organización y el el daño que pueda ocurrir a otros debe ser parte de la evaluación si el riesgo se debe vincular responsablemente con el potencial de daño, y si la evaluación debe ser comprensible para los reguladores y legales autoridades.

Las organizaciones también deberían considerar tener más de tres tipos de impacto en su impacto definiciones si tienen más de una misión, múltiples objetivos y muchas obligaciones que deben tener en cuenta en su análisis de riesgos. Si bien esta expansión puede crear una creciente amplio registro de riesgos, puede ayudar a las organizaciones a sentirse cómodas todos los intereses relevantes fueron considerado en su análisis de riesgos.

Las organizaciones de Nivel 3 y Nivel 4 que anteriormente usaban procesos de análisis de riesgos de Nivel 1 pueden aprovechar sus criterios de evaluación de riesgos más simples que usaban tres niveles de puntuación de impacto. Con el propósito de referencia a nuestra organización de ejemplo, un proveedor de información de salud, han pasado por una año o dos de gestión de riesgos, han ganado la atención y la confianza de los gerentes de negocios y ejecutivos. Como resultado, su capacidad para evaluar el riesgo de ciberseguridad utilizando criterios comerciales También mejorar.

Página 100

Podemos ver comparando los criterios de evaluación de riesgos para organizaciones de Nivel 1 en el Capítulo 2 con Tabla 57 que las descripciones detalladas de los impactos han aumentado en dos dimensiones; el número de las opciones de puntuación de impacto aumentaron de tres a cinco, y hay una definición de impacto adicional para objetivos comerciales.

Las organizaciones de Nivel 3 y Nivel 4 descubrirán que usar un rango de cinco puntajes aumenta la utilidad de priorización de riesgos al final de la evaluación de riesgos. Un criterio de evaluación de riesgos de tres por tres el modelo proporciona a las organizaciones seis posibles puntajes de riesgo; 1, 2, 3, 4, 6 y 9. Esto lleva a una agrupación de cursos que puede causar riesgos de urgencias algo diferentes indistinguible.

Un modelo de criterios de evaluación de riesgos de cinco por cinco permite 14 posibles puntuaciones de riesgo de; 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 20 y 25. Ahora es probable que se clasifiquen los riesgos de urgencias algo diferentes en diferentes puntajes de riesgo y se distinguirán más fácilmente al priorizarlos.

También tenga en cuenta que los puntajes de impacto de '1' y '2' en la Tabla 57 están sombreados en gris para separarlos de las puntuaciones más altas Los puntajes '1' y '2' describen las magnitudes de impacto que generalmente se pensarían de como aceptable. El proceso de criterios de aceptación de riesgos se explicará más adelante en el documento, pero Es útil considerar ahora que los puntajes '1' y '2' son consistentes en su definición de impacto magnitudes, y que las puntuaciones de impacto de '3', '4' o '5' podrían considerarse consistentemente como inaceptablemente alto.

Cuando el proveedor de información de salud de ejemplo se gradúa de usar sus instrucciones de Nivel 1, eso También tiene un nuevo tipo de impacto a considerar. La Tabla 57 usa un tipo de impacto para que los objetivos comerciales ser considerado en el análisis de riesgos de la organización. Los objetivos comerciales están más centrados en sí mismos que misiones y obligaciones, y están alineados con los criterios de éxito comúnmente encontrados en los negocios. Algunos ejemplos incluyen rentabilidad, crecimiento, mantenimiento de acreditaciones, satisfacción del cliente o retener una posición en el mercado.

Los objetivos se alinean más directamente con lo que comúnmente se considera el "costo" de una salvaguardia. Pero en lugar de permitir que una organización decida arbitrariamente que una salvaguarda cuesta demasiado, esto El método de incluir el costo en términos de impactos a los objetivos obliga a la organización a evaluar por qué Un costo sería excesivo. ¿El costo de la salvaguardia impide los objetivos de rentabilidad? Hace el salvaguardar la eficiencia o el crecimiento del límite? Esas son ciertamente preocupaciones razonables, siempre que Los objetivos de rentabilidad están a la par con el impacto de la misión y las obligaciones. *En otras palabras, un la organización no debería permitir que la rentabilidad sea más importante que dañar a otros o dañar a sus capacidad para cumplir su misión.*

Consulte la "Nota sobre el uso de los costos financieros como objetivos" en el Capítulo 5.

Figura 17 - Objetivos, misión, obligaciones

Objetivos	Misión	Obligaciones
• Auto beneficio	• Beneficio mutuo	• Beneficio de otros
• Riesgo propio	• riesgo mutuo	• Riesgo de otros

Las organizaciones están bien atendidas con este modelo porque la gestión empresarial, los técnicos, El personal de cumplimiento y el asesor legal tienen sus intereses abordados en el análisis de riesgos que usa estos criterios.

Page 101

Se proporciona una explicación detallada de cómo desarrollar definiciones de impacto con múltiples ejemplos en el capítulo "Técnicas de análisis de riesgos".

Definiciones de probabilidad

La definición de probabilidad para una organización de Nivel 3 y Nivel 4 también debería aumentar en matices a partir de la definición más simple de Nivel 1, y puede hacerlo agregando dos puntajes más a la tabla como se muestra en Tabla 58.

Tabla 58 - Ejemplos de definiciones de probabilidad

Probabilidad Puntuación	Previsibilidad
1	**No es previsible** . Esto no es plausible en el medio ambiente.
2	**Previsible** . Esto es plausible, pero no esperado.
3	**Esperado.** Estamos seguros de que esto eventualmente ocurrirá.
4 4	**Común.** Esto sucede repetidamente.
5 5	**Actual** . Esto puede estar sucediendo ahora.

- "No previsible" implica que una amenaza no es plausible en el entorno que se está juzgado. La pérdida de medios portátiles puede no ser previsible durante una evaluación de riesgos de un aplicación alojada
- "Previsible" implica algo plausible, pero la organización sería sorprendido si ocurrió. Un ejecutivo fundador que lleva copias de datos confidenciales a los competidores pueden considerarse previsibles, incluso si no se espera.
- “Esperado” implica una amenaza que no es común, pero que eventualmente sucedería. Se pueden esperar ataques de phishing u otros ataques de ingeniería social en muchos ambientes.
- "Común" implica algo que sucede repetidamente, como correos electrónicos mal dirigidos con información confidencial, ataques de malware o pérdida de computadoras portátiles y dispositivos móviles.
- "Actual" implica amenazas que rara vez no están presentes, como el escaneo de puertos en el perímetro dispositivos o compartir información en espacios cuasi públicos como mostradores de farmacia o cajeros de banco.

Cuando los evaluadores de riesgos estiman la probabilidad de una amenaza, seleccionarán los puntajes '1', 2 ',' 3 ',' 4 'o' 5 ' utilizando la definición de previsibilidad como su guía. Las organizaciones pueden agregar límites de tiempo en sus definiciones de previsibilidad (es decir, "previsible dentro de los umbrales de planificación", "esperado dentro del plan quinquenal "o" No previsible en el próximo año fiscal "). Si las organizaciones introducen el tiempo límites en sus definiciones de probabilidad, deben priorizar las inversiones de tratamiento de riesgos para cumplir con estos cronogramas Eso puede ser un desafío excesivo para muchas organizaciones, por lo que deben proceder con cuidado.

Desarrollo de los criterios de evaluación de riesgos.
Debido a que los criterios de evaluación de riesgos están destinados a describir el riesgo tal como se aplica a la organización que posee el riesgo, es apropiado para la alta gerencia que es responsable de
misión, objetivos y obligaciones de participar en el desarrollo y aceptación de los criterios.

La Tabla 59 enumera los roles comúnmente involucrados en el desarrollo de criterios de evaluación de riesgos, y el perspectiva interesada que aportan al esfuerzo de definición.

Tabla 59 - Roles involucrados en la definición de los criterios de evaluación de riesgos

Papel	Perspectiva
Director Ejecutivo Director de Operaciones	Asegurar que la misión, los objetivos y las obligaciones del organización están adecuadamente definidos, y para asegurar que un distinción entre impactos aceptables e inaceptables son debidamente delineado.
Director de Cumplimiento	Para asegurar que los intereses de las agencias reguladoras sean debidamente incluido en las definiciones de riesgo.
Director financiero	Para garantizar que los objetivos se definan adecuadamente, particularmente La distinción entre impactos aceptables e inaceptables.
Director de información Jefe de Tecnología	Para garantizar que el rendimiento técnico, el servicio y las capacidades se consideran e incluyen todo tipo de procesos de información más allá de la tecnología
Consejero general Abogado externo	Para garantizar que las obligaciones se definan adecuadamente y que comparar bien con la misión y los objetivos.
Auditoría interna Comité de Auditoría	Asegurar que las inquietudes de las partes interesadas estén bien representado en todas las definiciones de impacto y puntajes.
Clientes / clientes clave Constituyentes clave	Para asegurar que sus intereses estén incluidos en las obligaciones definición.

Ejercicio :

El lector puede desarrollar los criterios de evaluación de riesgos de su organización utilizando los "Criterios - Nivel Hoja de trabajo de 3 y 4 ”que se proporciona en el documento complementario *CIS_RAM_Workbook.*

El lector debe considerar:

1. Desarrollar los criterios de evaluación de riesgos en colaboración con gerentes de negocios. y asesoría legal para asegurar que las definiciones de Misión, Objetivos y Obligaciones son sensibles a la organización.
2. Trabajar con un asesor legal para ayudar a garantizar que las definiciones de impacto sean apropiadas abordar los intereses de todas las partes potencialmente afectadas y garantizar ese impacto Las declaraciones parecen equitativas para todas las partes.
3. Consulte la guía para definir y calificar los tipos de impacto en el "Análisis de riesgos Capítulo de Técnicas.

El evaluador de riesgos necesitará usar su juicio profesional para definir los tipos de impacto y describir los niveles de impacto que la organización debe lograr. Porque los criterios de evaluación de riesgos son una declaración de la organización de lo que lograrán en términos de daño a sí mismos y dañar a otros, las organizaciones deben consultar con un asesor legal antes de finalizar estos criterios y tomar decisiones de riesgo basadas en ellos.

Page 103

Definición de criterios de aceptación de riesgos

Introducción

Debido a que las evaluaciones de riesgo son esencialmente cuestiones de equilibrio, los criterios para aceptar el riesgo debería ayudar a determinar si se logró el equilibrio. En CIS la aceptación del riesgo RAM tiene dos componentes:

- Riesgo apropiado: que la probabilidad de un impacto debe ser aceptable para todos previsiblemente partes afectadas
- Riesgo razonable: que el riesgo planteado por una salvaguarda debe ser menor o igual al riesgo contra el que protege.

Si bien estos componentes se han demostrado brevemente anteriormente, el primer componente será descrito con más detalle en esta sección. El segundo componente se describirá más adelante en el Riesgo. Sección de recomendaciones de tratamiento más adelante.

Después de establecer las definiciones de impacto y probabilidad, las organizaciones de Nivel 3 y Nivel 4 ahora están bien posicionados para establecer sus criterios de aceptación de riesgos. Recordemos que los impactos se definieron dentro de puntajes que iban de '1' a '5'. Los puntajes de impacto aceptables '1' y '2' se definieron de una manera eso parecería apropiado para las partes interesadas (y está sombreado en gris para indicar su aceptabilidad), y el puntaje de impacto '3' fue el puntaje más bajo inaceptable.

Tabla 60 - Definiciones de impacto de ejemplo

Impacto Puntuación	Impacto a la misión	Impactar a Objetivos	Impacto a las obligaciones
	Misión: proporcionar información a ayudar a los pacientes remotos a permanecer saludable.	*Objetivo: operar rentable*	*Obligaciones: los pacientes no deben ser perjudicado por comprometido información.*
1	Los pacientes continúan accediendo información útil, y Los resultados van por buen camino.	Las ganancias están en el objetivo.	Los pacientes no experimentan pérdida de servicio o protección.
2	Algunos pacientes pueden no tener todo la información que necesitan como ellos lo solicitan.	Las ganancias están fuera del objetivo pero están dentro varianza planificada	Los pacientes pueden estar preocupados, pero no perjudicado
3	Algunos pacientes no pueden acceder la información que necesitan mantener buena salud resultados.	Las ganancias están apagadas varianza planificada y puede tomar un fiscal año para recuperarse.	Algunos pacientes pueden ser perjudicado financieramente o reputacionalmente después compromiso de información o servicios.
4 4	Muchos pacientes constantemente no puede acceder beneficioso información.	Las ganancias pueden tomar más que un fiscal año para recuperarse.	Muchos pacientes pueden ser perjudicado financieramente o reputacionalmente
5 5	Ya no podemos proporcionar información útil para el control remoto pacientes	La organización no puede operar rentable	Algunos pacientes pueden ser perjudicado financieramente, reputacional o fisicamente hasta e incluyendo la muerte.

Y de manera similar, los puntajes de probabilidad estuvieron dentro de un rango de '1' a '5' como se muestra a continuación. Una vez nuestro ejemplo la organización desarrolla su madurez de gestión de riesgos y está lista para refinar su riesgo distinciones, pueden decidir no tolerar impactos inaceptables si son *previsibles pero no esperado* ('2'), o si se *espera que ocurran* ('3'). Esta sería una decisión mejor tomada por su ejecutivos, y especialmente su equipo de cumplimiento, asesoría general y partes interesadas. Pero en En este caso, el modelo asumirá que seleccionó un puntaje umbral de '3'.

Tabla 61 - Ejemplos de definiciones de probabilidad

Probabilidad Puntuación	Previsibilidad
1	**No es previsible** . Esto no es plausible en el medio ambiente.
2	**Previsible** . Esto es plausible, pero no esperado.
3	**Esperado.** Estamos seguros de que esto eventualmente ocurrirá.
4 4	**Común.** Esto sucede repetidamente.
5 5	**Actual** . Esto puede estar sucediendo ahora.

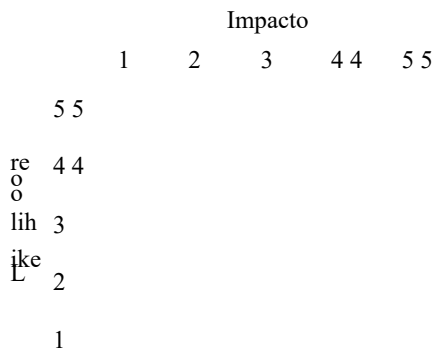
Por lo tanto, las organizaciones de Nivel 3 y Nivel 4 definirían su aceptación de riesgos de esta manera:

Tabla 62 - Criterios de aceptación de riesgos

Impacto Límite	X	Probabilidad Límite	=	Riesgo Límite
3	X	3	=	9 9
		… por lo tanto …		
Riesgo aceptable			<	9 9

A continuación se muestra un ejemplo del mapa de calor para este criterio de evaluación. Tenga en cuenta que este mapa de calor se define no solo por números y colores, sino ahora por un conjunto de criterios que abordan los negocios problemas y un deber de cuidado para proteger a los demás.

Figura 18 - Ejemplo de mapa de calor



Ejercicio :

El lector debe definir los criterios de aceptación de riesgos de su organización utilizando los "Criterios - Nivel Hoja de trabajo de 3 y 4 ”que se proporciona en el documento complementario *CIS_RAM_Workbook* .

El lector debe considerar:

1. Trabajar con un patrocinador de gestión empresarial que pueda ayudar a garantizar que el riesgo Los criterios de aceptación son sensibles para la organización.
2. Trabajar con un asesor legal para ayudar a garantizar que la definición de aceptación del riesgo aborda los intereses de todas las partes potencialmente afectadas y para garantizar ese impacto Las declaraciones parecen equitativas para todas las partes.

El evaluador de riesgos necesitará usar su juicio profesional para identificar niveles de riesgo aceptables. Debido a que los criterios de aceptación del riesgo son una declaración de la organización de lo que tolerarán en términos de daño a sí mismos y daño a otros, las organizaciones deben consultar con un asesor legal antes de finalizar estos criterios y tomar decisiones de riesgo basadas en ellos.

A medida que las organizaciones evalúan su riesgo utilizando los Controles CIS V7 (modelados en la siguiente sección), podrá determinar automáticamente si el riesgo se evalúa como aceptable o no sin necesitando considerar la pregunta de manera diferente en cada caso. Una simple estimación de la probabilidad e impacto determinará automáticamente cómo la organización debe priorizar cada riesgo, y si la organización puede aceptar el riesgo de manera segura como una opción "razonable".

Un proceso de evaluación de riesgos basado en amenazas

Introducción

Las organizaciones de nivel 3 y nivel 4 se benefician de la colaboración con la gestión empresarial. Ellos también Tener un conocimiento refinado de cómo funcionan los ciberataques. Y debido a su contacto con terceros tener considerablemente más datos sobre la efectividad en el terreno de sus salvaguardas de seguridad. Debido a que las organizaciones de Nivel 3 y Nivel 4 tienen estas ventajas, su capacidad para analizar y responder al riesgo debe ser más refinado que sus pares con menos madurez.

El método de análisis de riesgos descrito en esta sección se basa en un modelo de "ruta de ataque". Un ataque ruta, a veces llamada "cadena de muerte", es la ruta que toma un ataque para comprometer la información bienes. Por ejemplo, los ataques de ransomware implican muchas etapas de ataque, comenzando desde el hacker reconocimiento, a través de la preparación y entrega de exploits, compromiso inicial, abuso de privilegios, hasta el control final del volumen de almacenamiento y los datos de destino.

Y aunque no todos los ataques están planeados (algunos son automatizados, ataques automáticos, y otros son accidental) se pueden modelar en una ruta de ataque para comprender qué cadena de salvaguardas fallar para que una amenaza comprometa con éxito un activo.

La ruta de ataque para el ejemplo de ransomware anterior comenzaría con el atacante apuntando a un organización que probablemente pagaría un rescate para acceder a su información crítica. Lo harían investigar al personal clave de la organización para refinar su objetivo, y luego desarrollaría un explotar para ese personal. Pueden colocar el exploit en un servidor de Internet que sea accesible para la víctima, y elaboraría un mensaje de correo electrónico para la víctima que se vincule al exploit. Cuando el la víctima interactúa con el mensaje de correo electrónico, descargarían el ransomware que luego correr en su computadora. El atacante podría usar el ransomware para cifrar el disco duro, y dependiendo de la variación del ransomware, bloquee la información o cópiela en Internet servidor que controla el atacante.

Esta ruta de ataque se puede dibujar para incluir un conjunto de activos de información que la organización podría control, y eso sería explotado en el ataque, como; información sobre sus empleados y sus trabajos, servidores de correo electrónico, clientes de correo electrónico, firewalls, filtros de contenido, servidores proxy, protección contra malware electrodomésticos y software, sistemas operativos, discos duros, y sí, personas.

Figura 19 - Ejemplo de ruta de ataque y activos de información

Utilizando los pasos de análisis de riesgos que se describieron previamente para las organizaciones de Nivel 1 y Nivel 2, un El evaluador de riesgos puede utilizar el análisis de riesgos para determinar qué tan bien preparado está cada activo de información para prevenir o detectar ataques específicos mientras están en juego.

Este enfoque de "ruta de ataque" para el análisis de riesgos requiere un paso de análisis preliminar antes de trabajar en El registro de riesgos. Ese paso de análisis, el modelado de la ruta de ataque, documenta el ciclo de vida de un ataque, e identifica activos de información o clases de activos que estarían involucrados en el ataque. los La información desarrollada en este análisis preliminar proporciona al evaluador de riesgos una lista de activos de información que estarían involucrados en un tipo de ataque, y permite al evaluador evaluar los riesgos que enfrentan según cuán bien se alinean sus salvaguardas con los controles de la CEI.

Esta sección describirá y trabajará a través del análisis de ruta de ataque de una organización de Nivel 3 y Nivel 4 y registro de riesgos utilizando los Controles CIS para modelar salvaguardas apropiadas al riesgo. El registro de riesgos. y la hoja de trabajo del modelo de ruta de ataque descrita en esta sección están disponibles como plantillas en el documento complementario *CIS_RAM_Workbook* .

El registro de riesgos

El registro de riesgos de la organización Tier 3 y Tier 4 es muy similar al diseño de los registros de riesgos se muestra en las instrucciones de Nivel 1 y Nivel 2, pero establece modelos de ruta de ataque y amenazas como base para el análisis. Esta sección demostrará los procesos de evaluación de riesgos para el Nivel 3 y Organizaciones de nivel 4 que utilizan la plantilla de registro de riesgos provista en el documento complementario *CIS_RAM_Workbook* para *organizaciones* de Nivel 3 y Nivel 4.

El mapa de diseño de un registro de riesgos para una organización de Nivel 3 y Nivel 4 se muestra en la Figura 20.

Figura 20 - Mapa de diseño del registro de riesgos

El registro de riesgos para organizaciones de Nivel 3 y Nivel 4 es una lista de riesgos identificados y sus tratamientos de riesgo recomendados, también conocidos como "salvaguardas". Cada fila representa un riesgo y su recomendación de tratamiento de riesgo. Las partes del registro de riesgos son:

A. Los encabezados de columna y el texto guía para ayudar al lector o al evaluador de riesgos a comprender el información contenida en la columna.
B. Modelos de ataque y amenazas que son acciones dentro de una ruta de ataque.
C. Los activos de información dentro de la ruta de ataque que se están analizando.
D. El texto de Controles CIS que ayuda al evaluador de riesgos a considerar los controles que deberían estar en lugar para proteger los activos de información en el contexto de la ruta de ataque.
E. Cómo implementa la organización el Control CIS (si lo hacen) para proteger la información activo y cualquier vulnerabilidad que permita que la amenaza comprometa el activo.
F. La evaluación de riesgos, incluida la probabilidad de que la amenaza tenga éxito, los impactos a la misión, objetivos y obligaciones, si lo hizo, y el puntaje de riesgo resultante.
G. La implementación recomendada de los Controles CIS que reducirían los riesgos para un nivel aceptable, y el cálculo del riesgo de salvaguarda para estimar el riesgo de ese recomendación.

Modelos de ruta de ataque

La organización de Nivel 3 y Nivel 4 desarrollará un conjunto de modelos de ruta de ataque para documentar el pasos detallados que seguirían los ataques previsibles e identificar los activos de información que estaría involucrado en ese camino de ataque. Esto ayuda al evaluador de riesgos a evaluar los riesgos en función de cómo Las amenazas previsibles se comportan. El modelo de ruta de ataque permite a los evaluadores de riesgos hacer preguntas como, "Qué tan bien posicionados estamos frente a este tipo de ataque", "¿Estoy pensando en amenazas a los activos que como lo haría un atacante? ”y“ ¿Mi evaluación de riesgo para este activo se basa en la probabilidad y impacto de otros activos de información que estarían involucrados en el ataque?

La hoja de trabajo de modelos de ruta de ataque que utilizarán los evaluadores de riesgos para diseñar rutas de ataque se basa en El *modelo de ataque comunitario de CIS* , un documento proporcionado por CIS ® que asocia los controles de CIS con las etapas de planificación, detección y defensa de ciberseguridad. Esta sección demostrará el proceso para modelar rutas de ataque que los evaluadores usarán para analizar riesgos en el Nivel 3 y Registro de riesgos de la organización de nivel 4. Se proporciona una plantilla y ejemplos de este proceso en el documento complementario *CIS_RAM_Workbook* .

108

La hoja de trabajo de modelos de ruta de ataque se muestra en la Figura 21.

Figura 21 - Modelos de ruta de ataque

Modelo de ataque comunitario

Modelo de ruta de ataque

La hoja de trabajo de modelos de ruta de ataque consta de dos partes principales; el modelo de ataque comunitario en la parte superior, y los modelos de ruta de ataque en la parte inferior. El modelo de ataque comunitario anterior muestra Las etapas de un ataque en relación con los Controles CIS que podrían prevenir o detectar cada etapa.
Los modelos de ruta de ataque a continuación enumeran los tipos de incidentes de seguridad de la información que pueden ocurrir, y Identificar qué acciones y activos de información estarían involucrados en cada etapa del incidente.

El proceso
El evaluador de riesgos comenzará su evaluación modelando rutas de ataque en el modelo de ruta de ataque hoja de cálculo. La hoja de trabajo dará como resultado un conjunto de modelos de ruta de ataque (una fila por modelo), y Indique las acciones y los activos que pueden estar involucrados en cada ataque.

El evaluador de riesgos utilizará el registro de riesgos para analizar cada ruta de ataque (una etapa en el ruta de ataque por fila en el registro de riesgos). El evaluador evaluará cada etapa de una ruta de ataque. tal como analizarían cada riesgo en las evaluaciones de Nivel 1 y Nivel 2.

Las organizaciones de Nivel 3 y Nivel 4 pueden querer comenzar su análisis de riesgos analizando primero los riesgos utilizando los procesos descritos para organizaciones de Nivel 1 o Nivel 2, luego examinando amenazas específicas en una base de ruta de ataque. Esto asegura que todos los activos de información dentro del alcance y todos los Controles CIS serán abordado en el registro de riesgos, junto con los riesgos más específicos y detallados que se analizan utilizando este proceso basado en amenazas.

Page 109

Figura 22: Proceso de análisis de riesgos para organizaciones de nivel 3 y nivel 4

El proceso de evaluación de riesgos para las organizaciones de Nivel 3 y Nivel 4 asegura que los activos de información se analizan en términos del riesgo que plantean cuando se producen ataques multifase en el medio ambiente.
Este análisis basado en amenazas se realiza siguiendo los pasos que se detallan a continuación:

1. Usando la hoja de trabajo Modelo de ruta de ataque, el evaluador de riesgos crea una nueva fila en el hoja de trabajo para nombrar un tipo de ataque de seguridad cibernética o incidente de seguridad, como "Datos incautación a través de la aplicación web "o" Entrega incorrecta de información del paciente ".
2. El evaluador de riesgos luego se mueve a la derecha a través de la nueva fila para describir cada etapa de la ataque o incidente. La descripción incluiría un activo de información afectado y cómo el ataque comprometería el activo en cada etapa.
3. El evaluador de riesgos puede referirse a cada celda a través de una fila de ruta de ataque para poblar un riesgo registro. El evaluador de riesgos puede copiar el nombre del modelo de la ruta de ataque, las amenazas y activos de información que están en cada fila de modelo de ruta de ataque al registro de riesgos, con uno fila por modelo / amenaza / agrupación de activos.
4. Al considerar los controles que deben abordarse en cada fila del registro de riesgos, el evaluador de riesgos debe consultar la cuadrícula del Modelo de ataque comunitario en la parte superior del Ataque Hoja de trabajo del modelo de ruta para determinar qué controles deben estar en su lugar para detectar o prevenir la amenaza.
5. El evaluador de riesgos luego revisará los Controles CIS listados en cada fila del registro de riesgos, y reunirá evidencia de qué tan bien cada activo está protegido por salvaguardas asociado con el control CIS.

a. La evidencia puede ser en forma de entrevistas, una revisión de configuraciones o una revisión de registros y registros.

6. El evaluador de riesgos luego describirá cómo se aplica el control al activo de información o clase de activo en la celda "Control actual" de esa fila.
7. Luego, el evaluador considerará la diferencia entre el Control CIS y el actual salvaguarda aplicada para determinar si hay una deficiencia en cómo es el control Actualmente implementado y en funcionamiento. Si la salvaguardia actual no se implementa como descrito o de una manera que probablemente sea deficiente contra la amenaza, entonces el evaluador declarará Esto como una vulnerabilidad.
    a. Los evaluadores de riesgos deben considerar el objetivo del Control CIS al analizar riesgos Por ejemplo, CIS Control 16.11 establece "Bloquear automáticamente la estación de trabajo sesiones después de un período estándar de inactividad ". El objetivo del control es evitar que personas no autorizadas utilicen sesiones de usuario desatendidas. Si el actual el control no cumple el objetivo, entonces el evaluador debe indicar la brecha como un vulnerabilidad en la celda de vulnerabilidad, como: "Las estaciones de trabajo desatendidas pueden ser utilizado por personal que no tiene acceso autorizado a esos sistemas, o para aplicaciones que se asignan al usuario ausente ".
8. Ahora considere la amenaza que podría ocurrir debido a la vulnerabilidad.

Page 110

a. La vulnerabilidad anterior podría combinarse con esta amenaza: "Personal malintencionado puede abusar de los privilegios de los usuarios autorizados y puede ejecutar sin autorización transacciones o descargas de datos ".

9. Luego, calcule la probabilidad de que la amenaza tenga éxito y el impacto que puede crear.
    a. La estimación de probabilidad puede ser difícil, pero los criterios de evaluación de riesgos fueron desarrollado para proporcionar alguna orientación en ese proceso de estimación. La orientación es proporcionado en la sección Métodos para evaluar la probabilidad del "Análisis de riesgos Técnicas "más adelante en el documento
    si. Los puntajes de impacto deben proporcionar estimaciones del impacto que tal amenaza causaría crear. Considere las puntuaciones de probabilidad e impacto como un par. En otras palabras, "¿Cuál es la probabilidad de que resulte este impacto?" Proporcionar más orientación.
10. La puntuación de riesgo se calculará automáticamente en el registro de riesgos multiplicando el puntaje de probabilidad por el más alto de los tres puntajes de impacto.

Nivel 1 y Nivel 4 Evaluación de riesgos Ejemplo 1 - Ransomware en servidores de correo electrónico

La organización Tier 3 y Tier 4 ha expresado su preocupación por el ransomware y quiere saber cuál es su exposición a él. Quieren saber qué están haciendo ahora para evitar ransomware y qué otras inversiones necesitan hacer para estar apropiadamente protegido. Además, la organización está preocupada por dos vulnerabilidades de aplicaciones web, uno que permitiría la captura de datos, y el otro que permitirá la ejecución de código arbitrario a través de Sitios vulnerables. [19]

El evaluador de riesgos sabe considerar cada una de estas preocupaciones como modelos de ruta de ataque, y establece para documentar cada uno.

Al utilizar la hoja de trabajo Modelo de ruta de ataque, el evaluador de riesgos crea una fila titulada "Ransomware" y comienza a documentar la ruta de ataque como se muestra en la Tabla 63. La tabla se muestra en vertical formato para facilitar la visualización en este documento, pero está en formato horizontal en la plantilla proporcionada en *CIS_RAM_Workbook* .

Cada etapa de un modelo de ruta de ataque se describe utilizando el formato Modelo de ataque comunitario. por En cada etapa del modelo, el evaluador de riesgos describirá cómo el ataque comprometerá una activo de información.

[19] Este documento solo explorará cómo se definirá el primer modelo de ruta de ataque y el riesgo juzgado. Sin embargo, los otros dos escenarios se proporcionan en la hoja de trabajo Modelo de ruta de ataque como Otros ejemplos del proceso de modelado de la ruta de ataque.

Página 111

Tabla 63 - Modelo de ruta de ataque (ransomware)

Etapa de ruta de ataque	Acción de ruta de ataque
Modelo de ruta de ataque	Ransomware
Reconocimiento inicial	Los hackers determinan quién en la organización tiene acceso a información sensible. **Activo:** Información pública y sitios de redes sociales que Describir personal y responsabilidades.
Adquirir / Desarrollar herramientas	Los hackers moderadamente expertos pueden desarrollar correos electrónicos de phishing y explotaciones de ransomware que se dirigen al personal seleccionado. **Activo:** Fuera de nuestro control.
Entrega	El hacker envía correos electrónicos de phishing al personal seleccionado. **Activo:** servidor de correo electrónico, puerta de enlace SMTP.
Compromiso inicial	El personal abre el correo electrónico de phishing y activa una instalación de La carga útil del ransomware. **Activo:** cliente de correo electrónico, sistema operativo de usuario final, personal, proxy servidor.
Uso indebido / Privilegio de escalamiento	El malware cifra el volumen de almacenamiento local. **Activo** : SO del usuario final, volumen de almacenamiento.
Reconocimiento interno	No aplica
Movimiento lateral	No aplica
Establecer persistencia	Ver Uso indebido / Privilegio de escalamiento.
Ejecutar objetivos de misión	Los piratas informáticos requieren el pago por la devolución de la información para nosotros. **Activo:** efectivo o datos.

Como resultado de esta descripción detallada de la ruta de ataque, el evaluador de riesgos ahora puede detallar cada de estas etapas en el registro de riesgos como base de su análisis de riesgos. Entonces crean un conjunto de filas en su registro de riesgo que incluye la información que se muestra en el registro de riesgo parcial que se muestra en Tabla 64 y proporcionada más completamente en *CIS_RAM_Workbook* .

112

Tabla 64 - Registro de riesgo parcial con modelo de ruta de ataque

Camino de ataque Modelo	Amenaza	Activo de información
Ransomware Initial Recon: los hackers determinan	quien en la organización tiene acceso a información sensible.	Información pública y redes sociales. sitios que describen personal y responsabilidades.
Entrega de ransomware: el hacker envía phishing	correo electrónico al personal seleccionado.	Servidor de correo electrónico, puerta de enlace SMTP.
Compromiso inicial de ransomware: personal	abrir correo electrónico de phishing y activar una instalación del ransomware carga útil.	Cliente de correo electronico
Compromiso inicial de ransomware: personal	abrir correo electrónico de phishing y activar una instalación del ransomware carga útil.	SO del usuario final
Compromiso inicial de ransomware: personal	abrir correo electrónico de phishing y activar una instalación del ransomware carga útil.	Personal
Compromiso inicial de ransomware: personal	abrir correo electrónico de phishing y activar una instalación del ransomware carga útil.	Servidor proxy
Uso indebido de Ransomware / Privilegio de escalamiento:	El malware encripta el local volumen de almacenamiento	SO del usuario final
Uso indebido de Ransomware / Privilegio de escalamiento:	El malware encripta el local volumen de almacenamiento	Volumen de almacenamiento
Ransomware Ejecutar objetivos de misión:	Los hackers requieren pago por divulgación de información a nosotros.	Efectivo o datos

Cada fila en este registro de riesgos establece una relación entre el modelo de ruta de ataque (en este caso, "Ransomware"), una amenaza que podría ocurrir en cada etapa del ataque del ransomware, y el activo de información o clase de activo en el que ocurriría. Tenga en cuenta que los elementos etiquetados como "No aplicable" y "No está bajo nuestro control" en la Tabla 63 no se proporcionan filas en el registro de riesgo parcial en la Tabla 64. Esto es porque es poco lo que la organización puede hacer para abordar estos pasos en la ruta de ataque para escenario de ransomware.

También tenga en cuenta que muchos activos de información y muchos tipos de amenazas pueden considerarse dentro de un ruta de ataque El evaluador de riesgos debe determinar la cantidad de detalles y la variedad de activos / amenazas parejas que pretenden incluir en su evaluación. El modelado de la ruta de ataque puede tomar mucho hora. Debido a esto, los evaluadores de riesgos deberán considerar la cantidad de tiempo y recursos que tener disponible para realizar su análisis, y debe seleccionar un grado de detalle basado en eso

113

disponibilidad. Comenzar con activos obvios y amenazas para la primera evaluación puede ser suficiente, sabiendo que en evaluaciones posteriores se puede agregar más variedad al modelo.

Como resultado de este análisis, la organización busca en Internet menciones de privilegiados.
personal y sus roles. Quitan tanta información confidencial de esos sitios como
lata. Se dan cuenta de que hay otras formas de dirigirse al personal privilegiado, pero esto se considera un
paso prudente

El primer riesgo que el evaluador analiza en esta ruta de ataque es el uso del servidor de correo electrónico y
Puerta de enlace SMTP que puede recibir y retransmitir un mensaje de phishing a un usuario final objetivo. los
la organización cree que tienen buenas salvaguardas para manejar este riesgo, pero verifican el
Modelo de ataque comunitario para estar seguro.

Figura 23 - Selección de control CIS del modelo de ataque comunitario

Este riesgo se identificó en el modelo de ruta de ataque en la Tabla 63 en la etapa de "entrega", así que mientras
Evaluar el riesgo El evaluador de riesgos revisará el servidor de correo electrónico y la puerta de enlace SMTP debido a
su rol de entrega en el ataque, y los nombrará como activos en el registro de riesgos, como se muestra en
Tabla 64. A medida que el asesor haga referencia al Modelo de ataque comunitario, analizará el
intersección entre la columna *Entrega* y la fila *Proteger* para encontrar "Vulnerabilidad continua
evaluación "," firewall "," filtrado de pasarela de correo "," filtrado web "," acceso remoto seguro "y
"NIPS (sistema de prevención de intrusiones en la red)".

Teniendo en cuenta la amenaza del correo electrónico dirigido a usuarios específicos y el uso que hace la organización del correo electrónico
filtrando y sandboxing en su servidor corporativo, el evaluador de riesgos revisa los sub-controles bajo
Control CIS 7 "Protecciones de correo electrónico y navegador web". Entre esos subcontroles, el evaluador de riesgos
considera el Control 7.8 de CIS "Implementar DMARC y habilitar la verificación del lado del receptor" y CIS
Control 7.10 "Sandbox todos los archivos adjuntos de correo electrónico". Saben que los controles DMARC relacionados con CIS
El control 7.8 depende de una mayor cooperación comunitaria antes de que puedan ser confiables, e incluso entonces podrían
ser ignorado por determinados atacantes. También saben que determinados atacantes pueden pasar

114

las tecnologías de sandboxing de correo electrónico de la organización. Renuncian a analizar este riesgo porque también use antimalware en su servidor de correo electrónico y puerta de enlace SMTP, que aparece una fila hacia abajo la columna Entrega en la fila Detectar.

El evaluador de riesgos decide analizar el riesgo relacionado con su módulo de correo electrónico antimalware mediante haciendo referencia al CIS Control 8.1, como se describe en la Tabla 65.

Tabla 65 - Ejemplo de análisis de riesgos para el servidor de correo electrónico en un modelo de ruta de ataque de Ransomware

Ataque Ruta Modelo Ransomware	
Amenaza	Los piratas informáticos pueden atacar al personal que utiliza sus cuentas de correo electrónico personales, evitando así el servidor de correo electrónico corporativo.
Activo de información	Servidor de correo electrónico y puerta de enlace SMTP
Control CIS	8.1
Descripción	Utilice software antimalware administrado centralmente para continuamente supervisar y defender cada una de las estaciones de trabajo de la organización y servidores
Controlar	La detección y prevención avanzada de malware opera dentro del Puerta de enlace SMTP. Detecta y pone en cuarentena los archivos adjuntos y hipervínculos asociados con archivos maliciosos y sospechosos o URL bloqueadas
Vulnerabilidad	Los usuarios finales pueden ser víctimas de phishing por servicios de correo electrónico personal que pueden acceder desde las oficinas y en las computadoras del trabajo.
Probabilidad de amenaza	
Impacto de la misión	
Objetivos Impacto	
Obligaciones Impacto	
Puntuación de riesgo	
Aceptabilidad del riesgo	

Tenga en cuenta que el evaluador aún no ha evaluado este riesgo. Más bien, el evaluador de riesgos evaluará cada riesgo en la ruta de ataque después de considerar cómo ese conjunto de riesgos se afectan entre sí. Para nuestro ejemplo del modelo de ruta de ataque en la Tabla 63, los nueve riesgos se escribirán antes de que cada uno sea evaluado. Esto se hace para garantizar que la probabilidad y el impacto de cada riesgo se base en un escenario previsible, y no de forma aislada de cada activo, lo que puede causar algunos riesgos estimado arbitrariamente alto o bajo.

Trabajando más abajo en el modelo de ruta de ataque en la Tabla 63, la organización luego considera el riesgo pueden sufrir en clientes de correo electrónico de escritorio que se dirigen durante el *Compromiso Inicial* en este ruta de ataque de ransomware. Después de considerar la vulnerabilidad en el análisis de riesgo anterior que termina los usuarios aún pueden recibir mensajes de phishing a través de sus cuentas de correo electrónico personales, clientes de correo electrónico los riesgos están frescos en la mente del evaluador de riesgos. El evaluador de riesgos revisa el ataque comunitario Modelo en la Figura 24 para identificar controles CIS que se cruzan entre *Compromiso inicial* y *Protección* y ven que para esta etapa el anti-malware y CIS Control 8.1 es nuevamente un control apropiado para incluir en su evaluación. Describen el riesgo asociado con su implementación de CIS Control 8.1 en clientes de correo electrónico de escritorio en la Tabla 66.

Figura 24 - Selección de control CIS del modelo de ataque comunitario

Tabla 66 - Ejemplo de análisis de riesgos para el cliente de correo electrónico en un modelo de ruta de ataque de Ransomware

Modelo de ruta de ataque	Ransomware
Amenaza	El personal abre el correo electrónico de phishing y activa una instalación de Carga útil de ransomware. El correo electrónico puede ser recibido a través de personal cuentas de correo electrónico.
Activo de información	Cliente de correo electronico
Control CIS	8.1
Descripción	Utilice software antimalware administrado centralmente para continuamente supervisar y defender cada una de las estaciones de trabajo de la organización y servidores
Controlar	Antivirus basado en firmas en cada escritorio. Filtros antivirus URL web sospechosas utilizando un diccionario que se actualiza mensualmente.
Vulnerabilidad	La prevención avanzada de malware no está incluida en el punto final aplicaciones de protección en estaciones de trabajo de usuario final (que no sea URL filtración). Los usuarios finales pueden ser víctimas de phishing por correo electrónico personal servicios a los que pueden acceder desde oficinas y en computadoras de trabajo.
Probabilidad de amenaza	
Impacto de la misión	
Objetivos Impacto	
Obligaciones Impacto	
Puntuación de riesgo	
Aceptabilidad del riesgo	

Page 116

Este riesgo puede evaluarse como inaceptablemente alto cuando se considera todo el camino del ataque. Además, este riesgo parece ser independiente del primer riesgo que involucra al servidor de correo electrónico y Puerta de enlace SMTP. Tan robusto como el servidor SMTP corporativo puede ser para prevenir el ransomware phishing, al evaluador le preocupa que el riesgo de phishing de ransomware aún pueda ser inaceptablemente alto porque la puerta de enlace SMTP solo protege las cuentas de correo electrónico corporativas, no cuentas de correo electrónico personal alojadas por otros servicios.

El evaluador de riesgos nombró un servidor proxy como un activo de información en la etapa de "compromiso inicial" en el modelo de ruta de ataque en la Tabla 63 porque su servidor proxy bloquea las solicitudes de salida para direcciones IP y dominios con errores conocidos, incluidos hosts de malware conocidos. Entonces el evaluador de riesgos de nuevo hace referencia al modelo de ataque comunitario, mirando la columna *Compromiso inicial* y ve que la función de "filtrado web" del servidor proxy no está en esa columna. Además, el la organización no está utilizando los controles restantes en las filas *Proteger* y *Detectar* de esa columna, por lo que no pueden hacer referencia a esos controles en su columna "Controles actuales".

El modelo de ataque comunitario, aunque es muy útil para las organizaciones que modelan rutas de ataque,

es un documento de trabajo que se desarrollará constantemente a medida que cambien los comportamientos de amenaza y como controles cambiar para enfrentar nuevos desafíos. En el caso de esta organización, identifican el papel de un proxy servidor (una herramienta de filtrado web) para la *protección* contra el *compromiso inicial* de un ataque de malware. los El servidor proxy evita que el malware descargue la carga de un recurso web conocido como malo. Pero debido a que el Modelo de ataque comunitario no hace referencia al filtrado web en la intersección de *Protección* y *compromiso inicial* , la organización agrega ese control a esa célula. Ellos tienen identificó un caso para usar el filtro web para interrumpir el ransomware y debería registrarlo para el futuro utilizar.

El evaluador de riesgos decide evaluar el riesgo asociado con el servidor proxy para ver si pueden Ayudar a reducir el riesgo adecuadamente. El evaluador modela el riesgo en la Tabla 67.

Tabla 67 - Ejemplo de análisis de riesgos para el servidor proxy en un modelo de ruta de ataque de Ransomware

Ataque Ruta Modelo Ransomware	
Amenaza	El personal abre el correo electrónico de phishing y activa una instalación de Carga útil de ransomware. El correo electrónico puede ser recibido a través de personal cuentas de correo electrónico.
Activo de información	Servidor proxy
Control CIS	7.4
Descripción	Aplicar filtros de URL basados en la red que limitan la capacidad de un sistema para conectarse a sitios web no aprobados por la organización. Este filtrado se aplicará para cada uno de los sistemas de la organización, ya sea están físicamente en las instalaciones de una organización o no.
Controlar	Todo el tráfico de Internet para sistemas dentro de LAN corporativas y DMZ tiene URL filtradas contra un servicio de suscripción que bloquea sesiones con hosts mal conocidos y bloquea las URL no clasificadas como seguras por ese servicio
Vulnerabilidad	Las computadoras portátiles y dispositivos móviles omiten el servidor proxy cuando se usan fuera de la red corporativa. El ransomware puede atacar sistemas cuando están fuera de la red corporativa.
Probabilidad de amenaza	
Impacto de la misión	

Página 117

Ataque Ruta Modelo Ransomware
Objetivos Impacto
Obligaciones Impacto
Puntuación de riesgo
Aceptabilidad del riesgo

El evaluador de riesgos ve que el servidor proxy parece más robusto que la protección de punto final en sistemas de usuario final, pero aún tiene deficiencias. El servidor proxy no puede aplicar URL bloqueo en sistemas que no están en la red corporativa cuando un ataque de phishing ransomware ocurre.

Si bien los nueve riesgos en la ruta de ataque se evaluarían como un conjunto para la evaluación de riesgos real, Esta sección evaluará los tres riesgos de ejemplo para demostrar el proceso de evaluación grupal. El resto de los riesgos se evalúan completamente en la hoja de trabajo "Registro de riesgos - Nivel 3 y 4" en el *CIS_RAM_Workbook* .

Recuerde las definiciones de los puntajes de impacto y probabilidad que el Nivel 2, y el Nivel 3 y el Nivel 4 organizaciones creadas. Los puntajes de impacto se muestran en la Tabla 68.

Tabla 68 - Definiciones de impacto de ejemplo

Impacto Puntuación	Impacto a la misión	Impactar a Objetivos	Impacto a las obligaciones
	Proporcionar información para ayudar. Los pacientes remotos se mantienen saludables.	*Operar de manera rentable.*	*Los pacientes pueden sufrir daños si La información está comprometida.*
1	Los pacientes continúan accediendo información útil, y Los resultados van por buen camino.	Las ganancias están en el objetivo.	Los pacientes no experimentan pérdida de servicio o protección.
2	Algunos pacientes pueden no tener todo la información que necesitan como ellos lo solicitan.	Las ganancias están fuera del objetivo pero están dentro varianza planificada	Los pacientes pueden estar preocupados, pero no perjudicado
3	Algunos pacientes no pueden acceder la información que necesitan mantener buena salud resultados.	Las ganancias están apagadas varianza planificada y puede tomar un fiscal año para recuperarse.	Algunos pacientes pueden ser perjudicado financieramente o reputacionalmente después compromiso de información o servicios.
4 4	Muchos pacientes constantemente no puede acceder beneficioso información.	Las ganancias pueden tomar más que un fiscal año para recuperarse.	Muchos pacientes pueden ser perjudicado financieramente o reputacionalmente
5 5	Ya no podemos proporcionar información útil para el control remoto pacientes	La organización no puede operar rentable	Algunos pacientes pueden ser perjudicado financieramente, reputacional o físicamente hasta e incluyendo la muerte.

Las probabilidades se definieron de manera similar con cinco puntuaciones potenciales, como se muestra en la Tabla 69.

Tabla 69 - Ejemplos de definiciones de probabilidad

Probabilidad Puntuación	Previsibilidad
1	**No es previsible** . Esto no es plausible en el medio ambiente.
2	**Previsible** . Esto es plausible, pero no esperado.

118

Probabilidad Puntuación	Previsibilidad
3	**Esperado.** Estamos seguros de que esto eventualmente ocurrirá.
4 4	**Común.** Esto sucede repetidamente.
5 5	**Actual** . Esto puede estar sucediendo ahora.

La organización ahora volverá y revisará los riesgos asociados con el ataque de ransomware. ruta para estimar la probabilidad y el impacto de cada amenaza, pero en consideración de la otra riesgos de ransomware.

El evaluador de riesgos revisará esos riesgos en paralelo en la tabla abreviada a continuación.

Tabla 70 - Riesgos comparativos en un modelo de ruta de ataque de Ransomware

Camino de ataque Modelo	Ransomware		
Información Activo	Servidor de correo electrónico	Cliente de correo electronico	Servidor proxy
Amenaza	Los hackers pueden atacar al personal usando su correo electrónico personal cuentas, evitando así el Servidor de correo electrónico corporativo.	Personal abierto correo electrónico de phishing y desencadenar una instalación de Carga útil de ransomware. Email puede ser recibido a través de cuentas personales de correo electrónico.	Personal abierto correo electrónico de phishing y desencadenar una instalación de la Carga útil de ransomware. Email puede ser recibido a través de cuentas personales de correo electrónico.
Control CIS	8.1	8.1	7.4
Descripción	Utilice anti-gestión centralizada software malicioso para monitorear continuamente y defender cada uno de los estaciones de trabajo de la organización y servidores.	Utilice anti-gestión centralizada software malicioso para monitorear continuamente y defender cada uno de los estaciones de trabajo de la organización y servidores.	Aplicar URL basada en red filtros que limitan la capacidad de un sistema para conectarse a sitios web no aprobado por la organización. Este filtrado se aplicará para cada una de las organizaciones sistemas, ya sean físicamente en casa de una organización instalaciones o no.

Controlar	Detección avanzada de malware y la prevención opera dentro de La puerta de enlace SMTP. Detecta y archivos adjuntos de cuarentena e hipervínculos asociados con archivos maliciosos y sospechosos o URL bloqueadas.	Antivirus basado en firmas en cada escritorio Filtrado de URL web sospechosas que utilizan un diccionario que se actualiza mensual.	Todo el tráfico de Internet para sistemas dentro de LAN corporativas y DMZ tener URL filtradas contra un servicio de suscripción que bloquea sesiones con hosts mal conocidos, y bloquea las URL no categorizado como seguro por eso Servicio.
Vulnerabilidad	Los usuarios finales pueden ser víctimas de phishing por correo electrónico personal servicios a los que pueden acceder de oficinas y en el trabajo ordenadores.	Prevención avanzada de malware no está incluido en el punto final aplicaciones de protección en extremo estaciones de trabajo de usuario (que no sean Filtrado de URL). Los usuarios finales pueden ser víctimas de phishing servicios de correo electrónico personal que pueden acceder desde oficinas y en computadoras de trabajo.	Portátiles y dispositivos móviles omitir el servidor proxy cuando utilizado fuera de la LAN. El ransomware puede atacar sistemas cuando están fuera de La oficina LAN.
Amenaza Probabilidad	2	3	3
Misión Impacto	3	3	3
Objetivos Impacto	4 4	4 4	4 4

Page 119

Camino de ataque Modelo	Ransomware		
Obligaciones Impacto	4 4	4 4	4 4
Puntuación de riesgo	**8**	**12**	**12**
Riesgo Aceptabilidad	**Aceptable**	**Inaceptable**	**Inaceptable**

Después de evaluar cada uno de los riesgos en el modelo de ruta de ataque, el evaluador de riesgos (y, por extensión, su organización) se siente cómodo con la capacidad de la puerta de enlace SMTP para proteger a los usuarios de ataques de phishing de ransomware que pasan por el servidor de correo electrónico corporativo. Pero son menos cómodo con el riesgo de que esos ataques provengan de cuentas de correo electrónico personales mientras finalizan los usuarios usan sus computadoras portátiles lejos de la oficina. Los análisis de riesgos para el cliente de correo electrónico y el proxy los servidores son idénticos en este caso y se muestran en la Tabla 71.

Tabla 71 - Ejemplo de estimación de riesgo

Amenaza Probabilidad	Misión Impacto	Objetivos Impacto	Obligaciones Impacto	Puntuación de riesgo
3	3	4 4	4 4	12

El puntaje de riesgo es el producto del puntaje de probabilidad y el más alto de los tres puntajes de impacto, que en este caso es '3 x 4 = 12'.

Recuerde también que los criterios de aceptación de riesgos para la organización de Nivel 3 y Nivel 4 se ven así:

Tabla 72 - Criterios de aceptación del riesgo

Impacto Límite	X	Probabilidad Límite	=	Riesgo Límite
3	X	3	=	9 9
… por lo tanto …				
Riesgo aceptable			<	9 9

Un riesgo aceptable sería aquel que se evalúe a cualquier valor por debajo de '9'. Pero el riesgo de ransomware

es tan alto como '12' y, por lo tanto, es inaceptable.
Al analizar riesgos adicionales en la ruta de ataque del ransomware, como las protecciones en el usuario final
sistema operativo o volumen de almacenamiento, la organización puede mitigar aún más estos tres riesgos al
otras salvaguardas, como copias de seguridad de datos oportunas y confiables, o controles lógicos que impiden
los datos confidenciales son accedidos por las computadoras portátiles. Pero lo que se sabe es que, en términos de ransomware,
existe un riesgo continuo para la organización que no ha sido resuelto por la puerta de enlace SMTP
y servidor proxy.

120

Ejercicio :

El lector debe consultar la plantilla Registro de riesgos - Nivel 2 que se proporciona en el
documento complementario *CIS_RAM_Workbook.* Pueden usar la plantilla de registro de riesgos para
ingrese un conjunto de riesgos asociados con los modelos de ruta de ataque, controles CIS y
activos de información que están dentro del alcance de su evaluación.

Al hacer este ejercicio, el lector debe considerar:

1. Que el análisis basado en amenazas requiere un esfuerzo considerable y puede ser inverosímil como un
   Método para realizar una evaluación de riesgos completa e integral.
2. Realizar análisis basados en amenazas dentro de un registro de riesgos que se completó utilizando un
   Enfoque de Nivel 1 o Nivel 2. El análisis basado en amenazas puede usarse para responder a riesgos específicos
   preguntas como:
   a. Cuán realista es un puntaje de riesgo específico que parece exagerar o minimizar un
      riesgo independiente?
   si. ¿Existen riesgos que aún no hemos considerado en nuestro entorno?
   do. ¿Qué tan bien posicionados estamos para protegernos de una amenaza específica?
   re. ¿Cuál es la inversión más efectiva que podemos hacer para reducir un solo riesgo?
      que solo se realizaría dentro de una ruta de amenaza?
3. No "hirviendo el océano". No todos los activos se pueden evaluar prácticamente contra todos
   Controles CIS aplicables en una sola evaluación. Priorizar la evaluación de amenazas que
   parece más probable que otros, debido a experiencias pasadas u otras investigaciones.
4. Si un control o activo de información requiere un examen para comprender su valor real
   configuración y efectividad.
5. Si la organización puede tolerar la cantidad de esfuerzo y tiempo que el riesgo
   evaluación requiere.
   a. La organización debe usar análisis de alto nivel (revisión de políticas y
      entrevistas) si no tienen mucho tiempo y recursos.
   si. Los activos de información deben ser probados y examinados con más detalle a medida que pasa el tiempo.
      permite.
   do. La organización debe planificar evaluaciones de riesgos recurrentes para identificar más riesgos.
      a través del tiempo.
6. Colaborar con expertos en seguridad de la información para ayudar a modelar amenazas que son
   previsible en el medio ambiente, y para ayudar a evaluar la eficacia de la corriente
   salvaguardas

El evaluador de riesgos deberá usar su criterio profesional para seleccionar los controles y
activos de información y modelar amenazas que deben analizarse en la evaluación de riesgos.
Los expertos en seguridad de la información pueden necesitar ser incluidos en el proceso para asegurar que el riesgo
El análisis se realiza adecuadamente.

Resumen de evaluación de riesgos de nivel 3
Después de haber analizado un conjunto de riesgos contra un único activo de información, la organización de Nivel 2 se da cuenta de las ventajas de obtener una visión más completa de sus riesgos:

1. Modelar amenazas a través de rutas de ataque permite a las organizaciones de Nivel 3 y Nivel 4 evaluar los riesgos de ciberseguridad son más completos que al ver los activos de información individualmente.
2. El riesgo involucrado en un activo influirá en el riesgo de otros activos, que es más Imagen realista del riesgo dentro de un entorno en red.
3. Debido a que las rutas de ataque están alineadas con el Modelo de ataque comunitario, los evaluadores de riesgos son asistido por la comunidad de CIS en la identificación de los controles de CIS que son más adecuados para Prevenir y detectar ataques en varias etapas y activos en la ruta de ataque.

Después de evaluar los riesgos contra los activos de información, hemos identificado muchos que fueron inaceptablemente alto y eso debe proporcionarse con las garantías recomendadas para reducir su riesgo. Recorreremos e ilustraremos este proceso en las Recomendaciones de tratamiento de riesgos. sección a continuación.

Recomendaciones de tratamiento de riesgos

Introducción
Las organizaciones a menudo piensan en las salvaguardas de seguridad como obstáculos para los negocios y la productividad. Las salvaguardas a menudo hacen que el personal tome medidas adicionales para acceder a los sistemas o la información, o para obtener la aprobación de las actividades comerciales normales. Las salvaguardas requieren inversiones en tiempo y dinero, que compiten con otras prioridades. Y si se vuelven demasiado perjudiciales para la organización misión y objetivos, las salvaguardas de seguridad pueden ser desagradables y evitadas.

De hecho, las salvaguardias disruptivas a menudo hacen que el personal trabaje a su alrededor solo para obtener su trabajo hecho, lo que crea más riesgo.

Pero las recomendaciones de tratamiento de riesgo pueden y deben dar como resultado salvaguardas que sean demostrables razonable. Y mientras obtener una definición clara de "salvaguardas razonables" ha sido un desafío en las comunidades legales, regulatorias y de seguridad de la información, el CIS RAM proporciona un Solución práctica. Los evaluadores de riesgos evalúan las recomendaciones de tratamiento de riesgos para determinar si una salvaguarda de seguridad es razonable por; comparar la salvaguardia con el riesgo que se pretende reducir, y al comparar la salvaguarda con los criterios de aceptación del riesgo.

Las recomendaciones de tratamiento de riesgos son simples de evaluar una vez que los criterios de evaluación de riesgos y Se ha establecido un análisis de riesgo inicial. El proceso se realiza en los siguientes pasos:

1. Mientras examina un riesgo inaceptablemente alto, revise el Control CIS que corresponde con el riesgo y recomendar una forma factible para que la organización implemente o mejore ese controlar.
2. Si ese control no es factible en el corto plazo, recomiende otros controles CIS relacionados con El riesgo que se puede utilizar para reducirlo.
3. Evaluar el riesgo de la salvaguarda recomendada para comprender la carga que representaría a la organización. Luego compare ese riesgo de salvaguarda con los criterios de aceptación de riesgo para determinar si es apropiado
4. Compare también el riesgo evaluado de la salvaguarda recomendada con el riesgo observado para determinar si la salvaguarda es razonable (salvaguardas con puntajes de riesgo más bajos que los riesgos observados son razonables)
5. Clasifique los riesgos por su puntaje de riesgo para priorizar los riesgos y los tratamientos de riesgo que el la organización invertirá en

Esta sección muestra estos pasos en detalle al describir el proceso y luego al modelar el riesgo tratamientos para los riesgos inaceptablemente altos que se evaluaron en secciones anteriores.

Page 122

El lector debe revisar las definiciones de 'razonable' y 'apropiado' que se proporcionan en el glosario. Estos términos se usarán regularmente en esta sección y tienen significados distintos.

1. Apropiado: una condición en la cual los riesgos para los activos de información no previsiblemente crearán daño que es mayor que la organización o sus constituyentes pueden tolerar.
2. Razonable: una condición en la cual las salvaguardas no crearán una carga para la organización eso es mayor que el riesgo contra el cual está destinado a proteger.

Objetivos de tratamiento de riesgos

El objetivo de las recomendaciones de tratamiento de riesgos bien formadas es crear una lista priorizada de salvaguardas de seguridad de la información que proporcionarían protecciones apropiadas mientras no posan demasiado Una gran carga para el propósito de la organización.

Los ejercicios de recomendación de tratamiento de riesgo que se demuestran en esta sección examinan el riesgos inaceptables que se ilustraron anteriormente en el documento y seleccionarán los Controles CIS que reduciría esos riesgos en un grado que sea razonable (no excesivamente pesado) y apropiado (no inaceptablemente dañino).

Recomendaciones de salvaguardas de tratamiento de riesgos de los controles CIS V7

A medida que examinamos riesgos inaceptablemente altos, recomendaremos salvaguardas basadas en CIS Controles V7. Pero algunas de las salvaguardas que una organización está preparada para implementar y operar no puede implementarse exactamente como se describe en CIS Controls V7. Este proceso lleva en cuenta cómo seleccionar controles que aborden los riesgos y cómo determinar si son diseñado de una manera que tenga sentido en el contexto tanto del riesgo como de la carga potencial para el organización.

Recuerde la relación entre los riesgos analizados y sus tratamientos de riesgo recomendados en la Figura 25)

Figura 25 - Balance dentro del análisis de riesgo central

Un riesgo y su salvaguarda propuesta se evalúan utilizando el mismo criterio. Si un propuesto la salvaguarda tiene un riesgo más alto (su "riesgo de salvaguarda") que los criterios de aceptación del riesgo, entonces no es apropiado. Si la salvaguardia tiene una puntuación más alta que el riesgo observado, entonces no es razonable.

Los ejercicios en esta sección se centrarán en hacer coincidir los análisis de riesgo completados (en azul) con los nuevos garantías recomendadas (en verde).

123

Antecedentes: ¿qué tan realistas son las estimaciones de riesgo de salvaguarda?

Los lectores críticos se preguntarán cómo la organización y su asesor de riesgos sabrán si Sus estimaciones de riesgo de salvaguardia son realistas. Después de todo, ¿cómo pueden saber prospectivamente qué su riesgo estaría en tal situación?

Hay dos elementos importantes a tener en cuenta al obtener comodidad con esta práctica; Comprender las expectativas legales y regulatorias para la gestión de riesgos, y la información estándares de seguridad para evaluar las salvaguardas después de que se hayan implementado.

Ley y regulación: las leyes y regulaciones generalmente esperan que el análisis de riesgos evalúe salvaguardas que se requieren para lograr el cumplimiento, y se espera que el análisis de riesgos sea realizado por personas debidamente capacitadas e informadas. Estos análisis no garantizan seguridad que es suficiente contra cualquier amenaza, pero proporcionan un plan para mejorar seguridad y cumplimiento que se prioriza por la probabilidad de daño, y que no tiene intolerable daño como su objetivo.

Normas de gestión de riesgos de seguridad de la información: evaluación de riesgos de seguridad de la información Los estándares en los que se basa la RAM CIS operan dentro de programas de gestión de riesgos más completos y ciclos ISO 27005 opera dentro de la familia de estándares ISO 27000, y NIST 800-30 funciona dentro de las publicaciones especiales del NIST. Cada una de estas familias de estándares requiere continua análisis de salvaguardas de seguridad, incluido el análisis de controles después de que se hayan implementado para determinar si son efectivos para abordar sus objetivos de seguridad. Recomendado por lo tanto, las salvaguardas deben evaluarse nuevamente después de la implementación para asegurarse de que lograr sus objetivos previstos.

La organización Tier 3 y Tier 4 identificaron dos riesgos inaceptables al modelar un ransomware ruta de ataque sobre varios activos de información. El primero de estos riesgos inaceptables involucraba el correo electrónico. clientes que el personal utiliza para acceder al correo electrónico personal y cómo eso expone a la organización a ataques de phishing de ransomware. El riesgo se muestra nuevamente en la Tabla 73.

Tabla 73 - Ejemplo de análisis de riesgos para el cliente de correo electrónico en un modelo de ruta de ataque de Ransomware

Análisis de riesgo	Valor
Amenaza	El personal abre el correo electrónico de phishing y activa una instalación de Carga útil de ransomware. El correo electrónico puede ser recibido a través de personal cuentas de correo electrónico.
Activo de información	Cliente de correo electronico
Control CIS	8.1
Descripción	Utilice software antimalware administrado centralmente para continuamente supervisar y defender cada una de las estaciones de trabajo de la organización y servidores
Controlar	Antivirus basado en firmas en cada escritorio. Filtrado de sospechosos URLs web utilizando un diccionario que se actualiza mensualmente.
Vulnerabilidad	La prevención avanzada de malware no está incluida en el punto final aplicaciones de protección en estaciones de trabajo de usuario final (que no sea URL filtración). Los usuarios finales pueden ser víctimas de phishing por correo electrónico personal servicios a los que pueden acceder mientras trabajan desde casa usando el trabajo ordenadores.
Probabilidad de amenaza	3

Page 124

Análisis de riesgo	Valor
Impacto de la misión	3
Objetivos Impacto	4 4
Obligaciones Impacto	2

Puntuación de riesgo	**12**
Aceptabilidad del riesgo	**Inaceptable**

Pero debido a que este riesgo se identificó al evaluar una ruta de ataque, la organización considera las salvaguardas recomendadas en ese mismo contexto. Ellos comparan este riesgo con el otro riesgos inaceptables en la ruta de ataque en la Tabla 74 para determinar si una salvaguarda abordar ambos riesgos en el ataque. Ambos riesgos tienen el mismo puntaje de riesgo, pero por diferentes razones: Las computadoras portátiles no están protegidas contra malware avanzado a través del software de protección de punto final, y las computadoras portátiles no se benefician del servidor proxy mientras están fuera de la oficina.

Pueden agregar protección avanzada contra malware a sus puntos finales o pueden extender el servidor proxy a la DMZ y obligar a las computadoras portátiles a resolver consultas de red a través de ese servidor proxy mientras está fuera de la oficina.

Entonces modelan estas opciones a continuación.

Nota: El evaluador de riesgos registrará cómo abordarán su riesgo al indicar "Aceptar" "Reducir", "Transferir" o "Evitar". *Aceptar* y *reducir* riesgos será intuitivo para el lector. Un la organización puede *transferir* un riesgo mediante la contratación de un tercero que puede manejar el riesgo mejor, o mediante adquirir una póliza de seguro contra el riesgo. La organización también puede *evitar* el riesgo por no participar más tiempo en los procesos o manejar los activos de información que causan el riesgo

Tabla 74 - Riesgos comparativos en un modelo de ruta de ataque de Ransomware

Camino de ataque Modelo	**Ransomware**	
Activo de información	Cliente de correo electronico	Servidor proxy
Amenaza	El personal abre el correo electrónico de phishing y activa un instalación de carga útil de ransomware. Email puede ser recibido por correo electrónico personal cuentas	El personal abre el correo electrónico de phishing y activa un instalación de la carga útil del ransomware. Email puede ser recibido por correo electrónico personal cuentas
Control CIS	8.1	7.6
Descripción	Utilice anti-malware administrado centralmente software para monitorear y defender continuamente cada una de las estaciones de trabajo de la organización y servidores	Aplicar filtros de URL basados en la red que limitan un capacidad del sistema para conectarse a sitios web no aprobado por la organización. Este filtrado se aplicará para cada una de las organizaciones sistemas, ya sea físicamente en un instalaciones de la organización o no.
Controlar	Antivirus basado en firmas en cada escritorio. Filtrado de URL web sospechosas utilizando un diccionario que se actualiza mensualmente.	Todo el tráfico de Internet para sistemas dentro de empresas Las LAN y DMZ tienen URL filtradas contra un servicio de suscripción que bloquea sesiones con hosts mal conocidos y bloquea URL no categorizado como seguro por ese servicio.
Vulnerabilidad	La prevención avanzada de malware no está incluida en aplicaciones de protección de punto final en estaciones de trabajo de usuario (que no sean filtros de URL). Los usuarios finales pueden ser víctimas de phishing servicios de correo electrónico personal a los que pueden acceder desde oficinas y en computadoras de trabajo.	Las computadoras portátiles y dispositivos móviles omiten el proxy servidor cuando se usa fuera de la LAN. El ransomware puede atacar sistemas cuando están fuera de la oficina LAN.

Camino de ataque Modelo	**Ransomware**	
Probabilidad de amenaza	3	3
Impacto de la misión	3	3
Objetivos Impacto	4 4	4 4
Obligaciones Impacto	4 4	4 4
Puntuación de riesgo	**12**	**12**
Riesgo Aceptabilidad	**Inaceptable**	**Inaceptable**
Tratamiento de riesgo Opción	Reducir	Reducir

Recomendado Salvaguardia	Agregue un módulo de protección de malware avanzado a protección de punto final.	Extienda el servidor proxy a la DMZ y fuerce portátiles para usarlo como puerta de enlace.
Salvaguardar el riesgo	El costo inesperado estaría dentro del presupuesto plan de umbral si los módulos están restringidos a computadoras portátiles este año, y se extendió a las restantes sistema el año que viene. La amenaza del malware ya no sería esperado. Sin impacto en nuestra misión.	Las computadoras portátiles que usan VPN personales pueden omitir El servicio proxy. Si el servicio proxy no está disponible, puede causar los usuarios no deben usar los recursos de Internet mientras trabajando fuera de la oficina. Los servidores proxy no pueden detectar local ataques a los sistemas.
Amenaza de salvaguardia Probabilidad	2	3
Salvaguardia Impacto de la misión	1	2
Salvaguardia Objetivos Impacto	2	2
Salvaguardia Obligaciones Impacto	1	4 4
Salvaguardar el riesgo Puntuación	**4 4**	**12**
Salvaguardar el riesgo Aceptabilidad	**Aceptable**	**Inaceptable**

La organización de Nivel 3 y Nivel 4 ahora tiene la información que necesita para determinar y documentar por qué su salvaguarda recomendada es agregar prevención avanzada de malware en sus computadoras portátiles primero, luego escritorios en el siguiente año fiscal. Los escritorios estarán bien cubiertos por el servidor proxy cuando operado en su hogar permanente - la red de oficinas.

Page 126

Ejercicio :

El lector debe usar la plantilla "Registro de riesgos - Niveles 3 o 4" que se proporciona en el documento complementario *CIS_RAM_Workbook* para ingresar recomendaciones de tratamiento de riesgo para cada riesgo evaluado como inaceptablemente alto.

El lector debe considerar:

1. Si se puede mejorar una salvaguarda existente y cómo se haría.
2. Si una salvaguarda basada en un Control CIS diferente proporcionaría riesgo apropiado
3. Colaborar con expertos en temas de seguridad de la información para ayudar a modelar eficacia potencial de las salvaguardas recomendadas.

El evaluador de riesgos necesitará usar su juicio profesional para diseñar y recomendar salvaguardas de seguridad de la información y evaluar prospectivamente el riesgo que pueden presentar. Los expertos en seguridad de la información pueden necesitar ser incluidos en el proceso para asegurar que el riesgo El análisis se realiza adecuadamente.

Resumen de recomendaciones de tratamiento de riesgos

Las recomendaciones de tratamiento de riesgos son una parte crítica de la evaluación de riesgos para asegurarse de que La organización ha desarrollado un plan para abordar los riesgos sin crear otros riesgos para el organización o sus constituyentes. Algunos de los beneficios que se han demostrado sobre esto proceso son:

1. Las organizaciones pueden demostrar a los gerentes de negocios colaboradores cómo se recomienda se pueden implementar salvaguardas de seguridad sin gravar el propósito comercial evaluar el riesgo de las salvaguardas contra la misión y los objetivos de la organización.
2. Las organizaciones pueden demostrar a los reguladores y otras autoridades legales que las salvaguardas son razonables porque el riesgo esperado de la salvaguardia (la "carga" para el organización) no es mayor que el riesgo que reduce.
3. Las organizaciones pueden demostrar que las salvaguardas recomendadas serían "apropiadas" por mostrando que previsiblemente no crearían un impacto que sería intolerable para el organización o sus constituyentes.
4. Los tratamientos de riesgo recomendados pueden considerarse en términos de la ruta de ataque para el Nivel 3 y organizaciones de nivel 4. A medida que crece la madurez de las capacidades de seguridad de una organización, también lo hace la sofisticación y quizás la eficiencia de su tratamiento de riesgo recomendaciones

El proceso para evaluar riesgos y recomendar tratamientos de riesgo apropiados ha sido demostrado a nivel general. Sin embargo, algunas preguntas probablemente permanezcan para el lector evaluar salvaguardas, estimar probabilidad y la idoneidad de modelos de probabilidad en riesgo análisis. Estos temas más detallados se presentan en el próximo capítulo.

Page 127

Capítulo 5: Técnicas de análisis de riesgos

Las instrucciones, ejemplos y plantillas descritos en esta sección se entienden mejor a través de experiencia. El lector se beneficiará al usar los ejemplos que se proporcionan en el documento complementario *CIS_RAM_Workbook* para comprender mejor las instrucciones en este capítulo.

Técnicas de análisis de riesgos

Introducción

Los ejemplos de procesos de evaluación de riesgos descritos en este documento son ampliamente aplicables a Muchos casos y ambientes. Sin embargo, hay muchas razones por las cuales una organización modificar los procesos y plantillas que se proporcionan en la RAM CIS.

Métodos para estimar la probabilidad o probabilidad, evaluar salvaguardas y políticas, considerar riesgos de salvaguardas no técnicas y determinar qué riesgos evaluar o ignorar a todos los presentes Oportunidades para personalizar las evaluaciones de riesgos a entornos específicos.

Esta sección describe varios métodos de personalización para analizar los riesgos que las organizaciones pueden considerar como parte de sus evaluaciones de riesgos de ciberseguridad.

Definición de impactos para organizaciones de nivel 1

Quizás el primer paso más importante en la evaluación de riesgos es desarrollar un impacto efectivo definiciones La RAM CIS se basa en los principios del Análisis de Riesgos del Deber de Cuidados para permitir organizaciones para realizar evaluaciones de conciencia de su riesgo actual y previsto. Un riesgo La evaluación que resulta de la RAM CIS debería mostrar si las salvaguardas de seguridad de la información

son apropiados para el público, a la vez que son razonables para la organización. El núcleo de este análisis.
son las definiciones de impacto y el equilibrio y consenso que están destinados a establecer.

Esta sección proporcionará orientación para definir los tipos de impacto de manera efectiva.

Tabla 75 - Evaluación resumida de la definición de impacto

Beneficios	Límites
- Método consistente para evaluar el riesgo impactos. - Satisface el análisis de "costo-beneficio" que uso de reguladores. - Satisface la "prueba de equilibrio del deber de cuidado" que los tribunales confían - Equilibra los intereses comerciales con interés público.	- Las definiciones de impacto mal definidas pueden frustrar a los evaluadores de riesgos. - Definiciones de impacto pobremente "equilibradas" No puede reducir las responsabilidades legales.

El objetivo principal de las definiciones de impacto es proporcionar a los evaluadores de riesgos un método consistente para calificar riesgos que sean justos para todas las partes potencialmente afectadas. Una evaluación de riesgos debe demostrar tanta preocupación por la organización como por otros.

Para que esto sea posible, las definiciones de impacto deben diseñarse con el concepto de equilibrio firmemente en mente.

Recuerde las definiciones de impacto utilizadas para las organizaciones de Nivel 1 que se muestran en la Figura 26. Dos columnas abordar los intereses del propósito de la organización y las partes que pueden verse afectadas por

Page 128

riesgo de seguridad de la información. Cada una de estas columnas se considera un "tipo de impacto". El "Impacto para Nuestra misión "aborda el objetivo principal de las dos partes para imponer el riesgo ... el razón beneficiosa para que los clientes y la organización compartan información. La seguridad de la Los clientes pacientes de la organización se consideran en la columna "Impacto en las obligaciones".

Figura 26 - Ejemplos de definiciones de impacto

Ahora considere los puntajes de impacto y el límite rojo que separa el puntaje '1' de los puntajes '2' y '3'. Este límite marca la división entre impactos que presumiblemente serían aceptables. a todas las partes y a las que no lo serían.

Considere cómo los impactos para el puntaje '1' le parecerían a la organización, a los clientes pacientes y a los legales autoridades. La organización que utiliza esta definición de impacto afirma que aceptarían los impactos. de amenazas si resultan en condiciones similares a cómo se define el puntaje '1'. Esto indicaría que; los pacientes podrían acceder continuamente a la información que necesitaban, y los pacientes no ser previsiblemente perjudicados como resultado de una amenaza.

Luego considere cómo se definen los impactos para el puntaje '2'. Amenazas que previsiblemente resultarían en un el puntaje de impacto de '2' podría significar que algunos pacientes que no pueden acceder a la información pueden no mantener buenos resultados de salud. Ese escenario es claramente un impacto inaceptable para el misión de la organización, y no haría que valiera la pena que los pacientes confiaran su información con esa organización El puntaje de impacto de '2' para las obligaciones sería inaceptable porque previsiblemente, algunos de los pacientes pacientes podrían verse perjudicados financiera o reputacionalmente como resultado de un incidente, probablemente debido al robo de identidad o una interrupción del sistema.

Todas estas características de una definición de impacto lo hacen efectivo para estimar el riesgo de una manera que sea equitativo para todas las partes potencialmente afectadas, e incluso para impulsar el consenso dentro de la organización

que lo usa Después de todo, se abordan los intereses y el propósito de la organización, así como los intereses del público

Las organizaciones pueden construir definiciones de impacto efectivas definiendo cuidadosamente sus áreas de impacto, y luego definiendo cuidadosamente sus puntajes de impacto.

Definición de áreas de impacto

La RAM CIS describe dos áreas de impacto que deberían incluirse en el riesgo de una organización de Nivel 1 evaluación; Impacto a la misión e impacto a las obligaciones. Cada una de estas áreas de impacto aborda el intereses de personas u organizaciones que pueden verse afectadas por el riesgo de seguridad de la información. Cada uno desempeñar un papel significativo y único en el análisis de riesgos, y debe definirse dentro de esos roles, como descrito abajo.

Misión definitoria

Definición: La misión de una organización es el valor que proporciona a otros, y eso requiere que ellos participar juntos en el riesgo para lograr ese valor. Una universidad educa a sus estudiantes, pero los estudiantes deben dar información personal y financiera a esas universidades para recibir la educación.
Los minoristas ofrecen productos a los clientes, pero en muchos casos los clientes entregan sus información a esas organizaciones para recibir esos productos. Oferta de proveedores de servicios en la nube Funcionalidad basada en Internet para clientes comerciales, pero esos clientes deben entregar los negocios proceso u operaciones a esos servicios como resultado. Entonces "misión" es una forma de preguntar: "¿Qué hay en ella? para los demás? ", quienes se arriesgan con la organización.

Las definiciones de misión de ejemplo deben tener las siguientes características:

- Indique de manera concisa el beneficio que brinda la organización que alienta a otros a ordenar ellos en riesgo de seguridad de la información.
- Transmitir un hecho simple que puede ser observado y medido.
- Describa algo que la organización ya se las arregla y que el personal hará Reconocer como importante para la organización.

Ejemplo 1: un fabricante personalizado utiliza la propiedad intelectual de sus clientes para crear rápidamente componentes que son perfectos a la entrega. Su definición de misión puede ser: "Proporcionar clientes con productos que cumplen con sus especificaciones únicas, sin falta ". El mensaje es simple, se puede medir, y la organización probablemente reconoce esto como algo que ellos lograr Además, la definición puede ser útil cuando un evaluador de riesgos intenta determinar qué los valores centrales pueden verse perjudicados si existe un riesgo, o si una salvaguarda es demasiado gravosa para el misión. Si el evaluador de riesgos recomienda un control que evite que los clientes envíen sus capital intelectual, o que impide que el fabricante lo almacene o comparta entre los redactores e ingenieros, entonces la misión se vería claramente afectada negativamente.

Ejemplo 2: un banco comunitario declara su misión como: “Promovemos oportunidades para los hogares y pequeñas empresas al proporcionar productos financieros asequibles y servicios de asesoramiento ". podrían decir que su misión es prestar y pedir dinero prestado, pero están pensando en lo que no quieren comprometer esa misión, y eso es servir a su comunidad. Pero otra vez, tienen una definición concisa que establece por qué los demás se arriesgarían con ellos, que establece un hecho simple, observable y medible, y eso sería familiar para el personal que trabaja en el banco.

Ejemplo 3: se confía en gran medida en una empresa de telecomunicaciones para proporcionar comunicación servicios que ahora se consideran fundamentales para una sociedad en funcionamiento. Además, llevan enormes cantidades de información privada sobre sus clientes, a menudo a considerable riesgo percibido por el público. Pero los consumidores se suscriben a estos servicios para obtener un beneficio considerable. La compañía de telecomunicaciones define su misión de esta manera: "Instantaneamente y conectar de manera transparente a nuestros clientes con las personas, organizaciones, información y plataformas de comunicación que les interesan ". Esta definición de misión es menos concisa, pero puede ser lo más conciso posible, teniendo en cuenta la complejidad de las telecomunicaciones típicas servicios. La definición es medible y es muy probable que su personal la reconozca.

como un valor importante

Definición de obligaciones

Definición: Las obligaciones de una organización, al menos en términos de seguridad de la información, son prevenir daño previsible que puede llegar a otros como resultado de un compromiso de seguridad de la información. Estos tipos de daños se asocian comúnmente con el robo de identidad, el robo de fondos o la pérdida de servicios.

130

y datos. Pero es fundamental tener en cuenta que las obligaciones deben indicar explícitamente el daño que puede acudir a otros para que los evaluadores de riesgos, la gerencia y las partes interesadas sepan que La organización tiene cuidado de proteger a los demás del daño. Entonces, las "obligaciones" son una forma de preguntar: "¿Qué un daño previsible podría llegar a otros que deberíamos prevenir?

Una buena definición de obligaciones debe tener las siguientes características:

- Indique de manera concisa la intención de la organización de evitar daños a la seguridad de la información. Los incidentes pueden causar otros.
- Transmitir un hecho simple que puede ser observado y medido.
- Describa algo que la organización ya se las arregla y que el personal hará Reconocer como importante para la organización.

Ejemplo 1: el fabricante personalizado está preocupado por el daño que sus clientes pueden sufrir si su capital intelectual - sus diseños de productos - se filtran al público y al público competidores de los clientes. Sus clientes a menudo proporcionan especificaciones para componentes que Revelar secretos sobre nuevos productos. El fabricante declara sus obligaciones de esta manera: "Nuestro La propiedad intelectual de los clientes debe mantenerse confidencial para preservar su ventaja de mercado ". La definición es concisa, establece un daño previsible para otros que debe protegerse contra, t podría medirse, y el personal sabría que la protección de la propiedad intelectual de los clientes es importante.

Ejemplo 2: el banco comunitario sabe que sus clientes se encuentran en una situación particularmente vulnerable posición. A menudo asumen riesgos al comprar casas o iniciar negocios, y tienen menos margen de error Un sueldo perdido o incluso un mal uso de la información financiera podría significar diferencia entre el éxito y el fracaso para ellos. Entonces el banco comunitario usa esto como su definición de obligaciones, "Debemos proteger la reputación y el futuro financiero de nuestros clientes contra mal uso de su información financiera o personal ". Nuevamente, esta definición es concisa, es medible, y sería conocido y reconocido por el personal del banco.

Ejemplo 3: la compañía de telecomunicaciones es una organización compleja que puede imaginar múltiples tipos de daños que podrían resultar de un compromiso de seguridad de la información. Una organización con muchas obligaciones (o misiones u objetivos) pueden exponerlas en sus definiciones. Por ejemplo, la compañía de telecomunicaciones se da cuenta de que previsiblemente pueden violar personal comunicaciones sobre sus clientes y sus servicios de comunicación pueden fallar cuando es crítico Las aplicaciones dependen de ellos. Establecerán dos obligaciones: "Debemos proteger a nuestros clientes registros de comunicaciones para evitar daños a la reputación o financieros. Debemos cumplir con nuestro servicio acuerdos de nivel con los clientes para evitar daños que puedan resultar de una conectividad poco confiable ".

Como ejemplo, la fila superior de las definiciones de impacto para el fabricante comenzaría a tomar forma como en la tabla de abajo.

Tabla 76 - Ejemplo de definiciones de área de impacto (parcial)

Impacto a nuestra misión	Impacto a las obligaciones
Proporcionar a los clientes productos que cumplan Sus especificaciones únicas, sin falta.	*La propiedad intelectual de nuestros clientes debe ser mantenida confidencial para preservar su mercado ventaja.*

Página 131

Definición de puntajes de impacto

Después de definir las áreas de impacto, la organización deberá definir los puntajes de impacto para cada impacto zona. Cada puntaje ('1' a '3') tendrá una definición por área de impacto, como se muestra en la Figura 26. Hay algunos principios que las organizaciones deben considerar al definir sus puntajes de riesgo.

Considere que los puntajes tienen los siguientes significados:

Tabla 77 - Guía de puntuación de impacto

Impacto Puntuación	Dirección
1	Un impacto que sería aceptable para la misión, los objetivos y las obligaciones. Un el impacto sería notable, pero es probable que sea inevitable incluso después de una inversión significativa en controles. Sería considerado tolerable por todas las partes afectadas.
2	Un impacto que cualquier parte consideraría inaceptable. Si bien el impacto puede ser recuperable a través de esfuerzos adicionales, inversión o tiempo, la organización podría han reducido el riesgo de ese impacto con controles de seguridad.
3	El impacto sería catastrófico. La misión, objetivos y / u obligaciones Ya no será factible.

El puntaje '1' está sombreado para indicar que estos impactos deben definirse de una manera que sería aceptable para todas las partes.

A medida que se escriben las definiciones de puntaje de impacto, la organización debe pensar cómo impactan sus misión y obligaciones aparecerían en cada uno de estos niveles.

Las definiciones de puntaje de impacto del fabricante se muestran a continuación para ilustrar el punto.

Tabla 78 - Ejemplos de definiciones de puntaje de impacto

Puntaje de impacto	Impacto a nuestra misión	Impacto a las obligaciones
Definido	*Para proporcionar a los clientes productos que cumplen con sus especificaciones únicas, sin fallar.*	*Propiedad intelectual de nuestros clientes debe mantenerse confidencial para preservar su ventaja de mercado*
1	Los pedidos ocasionales no se pueden cumplir.	La información sobre trabajos puede ser conocido, pero nada que pueda dañar Posición de mercado de los clientes.
2	Los productos se entregan fuera de especificaciones y clientes creen que nosotros no puede producir productos personalizados sin fallar.	Un solo cliente experiencias repercusiones del mercado basadas en un incidente de seguridad
3	Ya no podemos producir productos confiables, Productos a medida.	Los clientes ya no pueden esperar protección de confidencialidad cuando trabajando con nosotros

Al leer una definición de impacto horizontalmente en una puntuación, tenga en cuenta que la definición de impacto en Cada área de impacto es igualmente perjudicial para todas las partes. Esta es una característica críticamente importante del deber de Análisis de riesgos asistenciales. Asegura que el análisis de riesgos sea equitativo. El daño de ninguna parte se considera más o menos tolerable que el daño de cualquier otra parte. Lo que es aceptable para uno equivale a lo que es

Page 132

aceptable para todos (la puntuación sombreada '1'). Lo que es catastrófico para uno equivale a lo que sería catastrófico para todos.

Las definiciones de impacto de ejemplo para las tres organizaciones de ejemplo se proporcionan en el documento complementario documento *CIS_RAM_Workbook* en la pestaña "Ejemplos de definiciones de impacto" para ayudar al lector comodidad y familiaridad con este tema.

Definición de impactos para organizaciones de nivel 2, nivel 3 y nivel 4

Quizás el primer paso más importante en la evaluación de riesgos es desarrollar un impacto efectivo definiciones La RAM CIS se basa en los principios del Análisis de Riesgos del Deber de Cuidados para permitir organizaciones para realizar evaluaciones de conciencia de su riesgo actual y previsto. Un riesgo La evaluación que resulta de la RAM CIS debería mostrar si las salvaguardas de seguridad de la información son apropiados para el público, a la vez que son razonables para la organización. El núcleo de este análisis. son las definiciones de impacto y el equilibrio y consenso que están destinados a establecer.

Esta sección proporcionará orientación para definir los tipos de impacto de manera efectiva.

Tabla 79 - Resumen de la evaluación de la definición de impacto

Beneficios	Límites
- Método consistente para evaluar el riesgo impactos. - Satisface el análisis de "costo-beneficio" que uso de reguladores. - Satisface la "prueba de equilibrio del deber de cuidado" que los tribunales confían - Equilibra los intereses comerciales con interés público.	- Las definiciones de impacto mal definidas pueden frustrar a los evaluadores de riesgos. - Definiciones de impacto pobremente "equilibradas" No puede reducir las responsabilidades legales.

El objetivo principal de las definiciones de impacto es proporcionar a los evaluadores de riesgos un método consistente para calificar riesgos que sean justos para todas las partes potencialmente afectadas. Una evaluación de riesgos debe demostrar tanta preocupación por la organización como por otros.

Para que esto sea posible, las definiciones de impacto deben diseñarse con el concepto de equilibrio firmemente en mente.

Recuerde las definiciones de impacto utilizadas para las organizaciones de Nivel 2, Nivel 3 y Nivel 4 que se muestran en la Figura 27. Tres columnas abordan los intereses de las partes que pueden verse afectadas por la seguridad de la información. riesgo. Cada una de estas columnas se considera un "tipo de impacto". La organización misma se considera mediante la evaluación de los posibles impactos en su capacidad de tener éxito en la columna "Impacto en los objetivos". La seguridad de los pacientes pacientes de la organización se considera en el "Impacto de las obligaciones" columna. Y la columna "Impacto en la misión" aborda el propósito principal para que las dos partes prohibir el riesgo ... la razón beneficiosa para que los clientes y la organización compartan información.

Figura 27 - Definiciones de impacto de ejemplo

Ahora considere los puntajes de impacto y el límite rojo que separa los puntajes '1' y '2' de puntajes '3', '4' y '5'. Este límite marca la división entre los impactos que presumiblemente ser aceptable para todas las partes y para aquellas que no lo serían.

Considere cómo los impactos para los puntajes '1' y '2' le parecerían a la organización, a los clientes pacientes, y autoridades legales. La organización que utiliza esta definición de impacto afirma que lo harían aceptar los impactos de las amenazas si resultan en condiciones similares a las puntuaciones '1' y '2' definido. Las amenazas que se califican con un impacto tan alto como '2' indicarían eso; no todos los pacientes recibirían la información que necesitaban, las ganancias estarían fuera del objetivo, pero dentro de lo planeado varianza, y los pacientes estarían preocupados por un incidente de seguridad, pero no sufrirían daños.

Luego considere cómo se definen los impactos para los puntajes de '3'. Amenazas que previsiblemente resultarían en una puntuación de impacto de '3' podría significar que algunos pacientes que no pueden acceder a la información pueden no mantener buenos resultados de salud. Ese escenario es claramente un impacto inaceptable para el misión de la organización, y no haría que valiera la pena que los pacientes confiaran su información con esa organización En términos de objetivos, la rentabilidad de la organización estaría fuera del plan y requeriría un año fiscal para recuperarse. Nuevamente, esto es inaceptable y debe invertirse. en contra para evitar el escenario. Y finalmente, el puntaje de impacto de '3' para las obligaciones sería inaceptable porque previsiblemente algunos de los pacientes pacientes podrían verse perjudicados financieramente o reputacionalmente como resultado de un incidente, probablemente debido al robo de identidad.

Todas estas características de una definición de impacto lo hacen efectivo para estimar el riesgo de una manera que sea equitativo para todas las partes potencialmente afectadas, e incluso para impulsar el consenso dentro de la organización que lo usa Después de todo, se abordan los intereses y el propósito de la organización, así como los intereses del público

Las organizaciones pueden construir definiciones de impacto efectivas definiendo cuidadosamente sus áreas de impacto, y luego definiendo cuidadosamente sus puntajes de impacto.

Definición de áreas de impacto

El CIS RAM describe tres áreas de impacto que deberían incluirse en la evaluación de riesgos; Impactar a Misión, impacto en los objetivos e impacto en las obligaciones. Cada una de estas áreas de impacto aborda el intereses de personas u organizaciones que pueden verse afectadas por el riesgo de seguridad de la información. Cada uno

desempeñar un papel significativo y único en el análisis de riesgos, y debe definirse dentro de esos roles, como descrito abajo.

Misión definitoria

Definición: La misión de una organización es el valor que proporciona a otros, y eso requiere que ellos participar juntos en el riesgo para lograr ese valor. Una universidad educa a sus estudiantes, pero los estudiantes deben dar información personal y financiera a esas universidades para recibir la educación.
Los minoristas ofrecen productos a los clientes, pero en muchos casos los clientes entregan sus información a esas organizaciones para recibir esos productos. Oferta de proveedores de servicios en la nube Funcionalidad basada en Internet para clientes comerciales, pero esos clientes deben entregar los negocios

proceso u operaciones a esos servicios como resultado. Entonces "misión" es una forma de preguntar: "¿Qué hay en ella? para los demás? ", quienes se arriesgan con la organización.

Las definiciones de misión de ejemplo deben tener las siguientes características:

- Indique de manera concisa el beneficio que brinda la organización que alienta a otros a ordenar ellos en riesgo de seguridad de la información.
- Transmitir un hecho simple que puede ser observado y medido.
- Describa algo que la organización ya se las arregla y que el personal hará Reconocer como importante para la organización.

Ejemplo 1: un fabricante personalizado utiliza la propiedad intelectual de sus clientes para crear rápidamente componentes que son perfectos a la entrega. Su definición de misión puede ser: "Proporcionar clientes con productos que cumplen con sus especificaciones únicas, sin falta ". El mensaje es simple, se puede medir, y la organización probablemente reconoce esto como algo que ellos lograr Además, la definición puede ser útil cuando un evaluador de riesgos intenta determinar qué los valores centrales pueden verse perjudicados si existe un riesgo, o si una salvaguarda es demasiado gravosa para el misión. Si el evaluador de riesgos recomienda un control que evite que los clientes envíen sus capital intelectual, o que impide que el fabricante lo almacene o comparta entre los redactores e ingenieros, entonces la misión se vería claramente afectada negativamente.

Ejemplo 2: un banco comunitario declara su misión como: “Promovemos oportunidades para los hogares y pequeñas empresas en nuestra comunidad al proporcionar productos financieros asequibles y asesoramiento servicios ". Podrían decir que su misión es prestar y pedir dinero prestado, pero están pensando antes de lo que no quieren comprometer sobre esa misión, y eso es servir a sus comunidad. Pero, de nuevo, tienen una definición concisa que establece por qué otros prohibirían el riesgo. con ellos, eso establece un hecho simple, observable y medible, y que sería familiar para personal que trabaja en el banco.

Ejemplo 3: se confía en gran medida en una empresa de telecomunicaciones para proporcionar comunicación servicios que ahora se consideran fundamentales para una sociedad en funcionamiento. Además, llevan enormes cantidades de información privada sobre sus clientes, a menudo a considerable riesgo percibido por el público. Pero los consumidores se suscriben a estos servicios para obtener un beneficio considerable. La compañía de telecomunicaciones define su misión de esta manera: "Instantaneamente y conectar de manera transparente a nuestros clientes con las personas, organizaciones, información y plataformas de comunicación que les interesan ". Esta definición de misión es menos concisa, pero puede ser lo más conciso posible, teniendo en cuenta la complejidad de las telecomunicaciones típicas servicios. La definición es medible y es muy probable que su personal la reconozca. como un valor importante

Definiendo objetivos

Definición: Los objetivos de una organización están más enfocados hacia adentro y son más egoístas. Como personas comúnmente piensan en la "carga" de una salvaguardia, a menudo piensan en "objetivos" y con mayor frecuencia en

135

carga financiera o "costo". Pero el costo es una métrica de riesgo excesivamente estrecha y potencialmente peligrosa. Las organizaciones deberían querer mantenerse alejadas del análisis que asocia cantidades financieras a niveles de daño que otros sufrirían. "No gastaremos $ 200,000 para proteger la privacidad de nuestros clientes", es Un mensaje terrible para enviar al personal, a los clientes y al público. Por el contrario, las organizaciones debe pensar en los indicadores de que están teniendo éxito o fallando como en la organización, independientemente de su definición de misión. Entonces, los "objetivos" son una forma de preguntar: "¿Cómo sabemos que somos un organización exitosa?

Una buena definición de objetivos debe tener las siguientes características:

- Indique de manera concisa los indicadores de éxito que sean independientes de la definición de la misión.
- Transmitir un hecho simple que puede ser observado y medido.
- Describa algo que la organización ya se las arregla y que el personal hará Reconocer como importante para la organización.

Ejemplo 1: el fabricante personalizado tiene un plan de cinco años para expandirse a dos nuevos mercados y cuadruplica su producción y ganancias. Saben no asociar dólares a posibles daños a otros, pero el crecimiento de la productividad y la rentabilidad todavía se pueden establecer adecuadamente como un objetivo. Su La definición de objetivos puede ser: "Cuadruplicar nuestra producción y ganancias en cinco años a través de expansión a dos nuevos mercados ". El mensaje es conciso e independiente de la misión, 20 latas ser observado y medido, y sería conocido por el personal, pero particularmente por la gerencia

cuyas metas estarían alineadas con el plan quinquenal.

Ejemplo 2: la misión del banco comunitario es convincente, y es posible que quieran asociarse
El éxito de su banco con el éxito de su comunidad. Pero deben funcionar como un viable
institución financiera si van a servir a los miembros de su comunidad. Entonces sus objetivos serán
dirigido a ese objetivo. Creen que necesitan mantener una cierta relación de retorno de activos para
compensar el riesgo financiero futuro y decirlo de esta manera: "Debemos retener una rentabilidad de los activos del 1,25%
año tras año ". Esta definición es un indicador conciso de éxito que se puede medir fácilmente, y
ese personal, y ciertamente gerentes y oficiales, ya estarían operando.

Ejemplo 3: la compañía de telecomunicaciones sabe muy bien una cosa; que independientemente de su
ganancias, su crecimiento en la base de consumidores, su crecimiento en inversiones de capital o su reputación ...
si caen por debajo de su estado de "dos mejores" en su mercado competitivo, serán el objetivo de
adquisición. Definen sus objetivos de esta manera: "Para aumentar nuestra base de suscriptores, las comunicaciones
capital e ingresos más rápido que nuestra competencia y seguir siendo el número uno o dos en el
mercado ". De nuevo, esto es menos conciso, pero la compañía depende de muchas partes móviles para ser
exitoso. La definición de los objetivos se puede medir, y el personal ciertamente es consciente de
objetivos y son responsables de gestionarlos.

Nota sobre el uso de los costos financieros como objetivos: organizaciones que desean declarar sus
impactos en términos de costos financieros deben considerar cuidadosamente el mensaje que envían a
colegas, partes interesadas y autoridades a medida que definen sus puntajes de impacto de objetivos. Si una
puntaje de impacto inaceptable ('3') para estados objetivos, por ejemplo, "$ 100,000", y lo mismo
el puntaje ('3') para las obligaciones es "Hasta 100 clientes recibirían el robo de su información y
abusado "o algo similar, entonces la organización dice:" No gastaríamos $ 100,000 para

[20] El éxito de los objetivos puede depender del éxito de la misión, pero el
La definición de los objetivos no depende de la definición de la misión.

Page 136

proteger a 100 clientes? ”Si es así, ¿están preparados para la manera en que sus colegas, el público y los legales
las autoridades percibirán ese mensaje?

Al centrarse en la magnitud de los impactos contra los objetivos (incluso la noble causa de rentabilidad
o desempeño financiero) en términos de daño a la organización (su capacidad para operar de manera rentable, o
recuperar la rentabilidad después de un evento) pueden presentar su balance de riesgo de manera responsable.

Este enfoque cualitativo para evaluar los impactos en los objetivos financieros sigue siendo útil al describir
el costo de las salvaguardas recomendadas y la evaluación de la magnitud que tendrá el costo en el
objetivos Tales comparaciones caso por caso aún establecerían el valor financiero de la propuesta
salvaguardar, pero ese valor financiero se compararía con un principal operativo llamado
"Rentabilidad" o "desempeño financiero" que las reglamentaciones y los tribunales ya incluyen en sus
definición de "carga".

Definición de obligaciones

Definición: Las obligaciones de una organización, al menos en términos de seguridad de la información, son prevenir
daño previsible que puede llegar a otros como resultado de un compromiso de seguridad de la información.
Estos tipos de daños se asocian comúnmente con el robo de identidad, el robo de fondos o la pérdida de servicios.
y datos. Pero es fundamental tener en cuenta que las obligaciones deben indicar explícitamente el daño que puede
acudir a otros para que los evaluadores de riesgos, la gerencia y las partes interesadas sepan que
La organización tiene cuidado de proteger a los demás del daño. Entonces, las "obligaciones" son una forma de preguntar: "¿Qué
un daño previsible podría llegar a otros que deberíamos prevenir?

Una buena definición de obligaciones debe tener las siguientes características:

- Indique de manera concisa la intención de la organización de evitar daños a la seguridad de la información.
  Los incidentes pueden causar otros.
- Transmitir un hecho simple que puede ser observado y medido.

• Describa algo que la organización ya se las arregla y que el personal hará Reconocer como importante para la organización.

Ejemplo 1: el fabricante personalizado está preocupado por el daño que sus clientes pueden sufrir si su capital intelectual - sus diseños de productos - se filtran al público competidores de los clientes. Sus clientes a menudo proporcionan especificaciones para componentes que Revelar secretos sobre nuevos productos. El fabricante declara sus obligaciones de esta manera: "Nuestro La propiedad intelectual de los clientes debe mantenerse confidencial para preservar su ventaja de mercado ". La definición es concisa, establece un daño previsible para otros que debe protegerse contra, t podría medirse, y el personal sabría que la protección de la propiedad intelectual de los clientes es importante.

Ejemplo 2: el banco comunitario sabe que sus clientes se encuentran en una situación particularmente vulnerable posición. A menudo asumen riesgos al comprar casas o iniciar negocios, y tienen menos margen de error Un sueldo perdido o incluso un mal uso de la información financiera podría significar diferencia entre el éxito y el fracaso para ellos. Entonces el banco comunitario usa esto como su definición de obligaciones, "Debemos proteger la reputación y el futuro financiero de nuestros clientes contra mal uso de su información financiera o personal ". Nuevamente, esta definición es concisa, es medible, y sería conocido y reconocido por el personal del banco.

Ejemplo 3: la compañía de telecomunicaciones es una organización compleja que puede imaginar múltiples tipos de daños que podrían resultar de un compromiso de seguridad de la información. Una organización con muchas obligaciones (o misiones u objetivos) pueden exponerlas en sus definiciones. Por ejemplo, la compañía de telecomunicaciones se da cuenta de que previsiblemente pueden violar personal comunicaciones sobre sus clientes y sus servicios de comunicación pueden fallar cuando es crítico Las aplicaciones dependen de ellos. Establecerán dos obligaciones: "Debemos proteger a nuestros clientes

137

registros de comunicaciones para evitar daños a la reputación o financieros. Debemos cumplir con nuestro servicio acuerdos de nivel con los clientes para evitar daños que puedan resultar de una conectividad poco confiable ".

Como ejemplo, la fila superior de las definiciones de impacto para el fabricante comenzaría a tomar forma como en la tabla de abajo.

Tabla 80 - Ejemplo de definiciones de área de impacto (parcial)

Impacto Puntuación	Impacto a nuestra misión	Impacto a los objetivos	Impacto a las obligaciones
	Para proporcionar a los clientes productos que cumplen con sus especificaciones únicas, sin fallar.	*Para cuadruplicar nuestro producción y ganancias en cinco años a través expansión en dos nuevos mercados*	*Intelectual de nuestros clientes la propiedad debe mantenerse confidencial para preservar su ventaja de mercado*

Definición de puntajes de impacto

Después de definir las áreas de impacto, la organización deberá definir los puntajes de impacto para cada impacto zona. Cada puntaje ('1' a '5') tendrá una definición por área de impacto, como se muestra en la Figura 27. Hay algunos principios que las organizaciones deben considerar al definir sus puntajes de riesgo.

Considere que los puntajes tienen los siguientes significados:

Tabla 81 - Guía de puntuación de impacto

Impacto Puntuación	Dirección
1	**Un impacto que sería insignificante para la misión, los objetivos y las obligaciones. Si ocurriera algún impacto, no sería notable.**
2	Un impacto que sería aceptable para la misión, los objetivos y las obligaciones. Un el impacto sería notable, pero es probable que sea inevitable incluso después de una inversión significativa en controles. Sería considerado tolerable por todas las partes afectadas.
3	Un impacto que cualquier parte consideraría inaceptable. Si bien el impacto puede ser recuperable a través de esfuerzos adicionales, inversión o tiempo, la organización podría han reducido el riesgo de ese impacto con controles de seguridad.

4 4	Un impacto que se consideraría grande, pero recuperable. Esfuerzos significativos y Se necesitarían inversiones para recuperar a todas las partes.
5 5	El impacto sería catastrófico. La misión, objetivos y / u obligaciones Ya no será factible.

Los puntajes '1' y '2' están sombreados para indicar que estos impactos deben definirse de una manera que Ser aceptable para todas las partes.

A medida que se escriben las definiciones de puntaje de impacto, la organización debe pensar cómo impactan sus misión, objetivos y obligaciones aparecerían en cada uno de estos niveles.

Las definiciones de puntaje de impacto del fabricante se muestran a continuación para ilustrar el punto.

Page 138

Tabla 82 - Definiciones de puntaje de impacto de ejemplo

Impacto Puntuación	Impacto a nuestra misión	Impacto a los objetivos	Impacto a las obligaciones
Definido	*Para proporcionar a los clientes productos que cumplen con sus especificaciones únicas, sin fallar.*	*Para cuadruplicar nuestro producción y ganancias en cinco años a través expansión en dos nuevos mercados*	*Intelectual de nuestros clientes la propiedad debe mantenerse confidencial para preservar su ventaja de mercado*
1	Los clientes reciben excelente productos, según sea necesario.	Nuestro plan de crecimiento permanece En el blanco.	Toda la propiedad intelectual es protegido.
2	Los pedidos ocasionales no pueden ser cumplido	Nuestros objetivos anuales están apagados año por año, pero dentro de varianza planificada	La información sobre trabajos puede ser conocido, pero nada que puede dañar a los clientes posición en el mercado
3	Trabajo contratado para pocos los clientes no pueden ser completado según lo planeado.	Nuestro crecimiento es demasiado bajo para un año, pero puede ser recuperado para cumplir con el objetivo de cinco años.	Información sobre un trabajo. fugas, y un cliente necesita investigar si creó daño. Incluso si el daño directo fuera No resulta.
4 4	Los productos se entregan afuera de especificaciones y clientes creen que no podemos producir Productos personalizados sin falta.	No podemos cumplir con los cinco plan de crecimiento anual.	Un solo cliente mercado de experiencias repercusiones basadas en un incidente de seguridad
5 5	Ya no podemos producir Productos confiables y personalizados.	No podemos operar rentable	Los clientes ya no pueden esperar confidencialidad protección al trabajar con nosotros.

Al leer una definición de impacto horizontalmente en una puntuación, tenga en cuenta que la definición de impacto en Cada área de impacto es igualmente perjudicial para todas las partes. Esta es una característica críticamente importante del deber de Análisis de riesgos asistenciales. Asegura que el análisis de riesgos sea equitativo. El daño de ninguna parte se considera más o menos tolerable que el daño de cualquier otra parte. Lo que es aceptable para uno equivale a lo que es aceptable para todos (las puntuaciones sombreadas '1' y '2'). Lo que es catastrófico para uno equivale a lo que Sería catastrófico para todos.

Las definiciones de impacto de ejemplo para las tres organizaciones de ejemplo se proporcionan en el documento complementario documento CIS_RAM_Workbook en la pestaña "Ejemplos de definiciones de impacto" para ayudar al lector comodidad y familiaridad con este tema.

Estimación de la probabilidad a través del análisis de "preparación para la defensa"

La RAM CIS presenta un método estandarizado para estimar la probabilidad de un incidente por centrándose en cómo una amenaza podría interactuar con una vulnerabilidad. Este concepto de previsibilidad es fácilmente comunicado a audiencias amplias, y está incrustado en lenguaje legal y regulatorio, por lo que es un constructo útil para la estimación de probabilidad. Sin embargo, algunas organizaciones necesitan más rigor mientras estimando la probabilidad y puede lograr eso evaluando las características de un éxito o ataque fallido en su entorno.

Tabla 83 - Resumen de la evaluación del análisis de preparación para la defensa

Beneficios	Límites
- Método consistente para evaluar la probabilidad - Apoya la estimación basada en evidencia	- No se basa en un estándar establecido - Los criterios basados en evidencia son opcionales

Tomando prestado del análisis de riesgo binario, [21] "análisis de preparación de defensa" hace una serie de preguntas sobre ataques y salvaguardas para estimar la capacidad de un control para detectar o prevenir lo previsible amenazas [22] Un evaluador de riesgos puede evaluar rápidamente la preparación para la defensa haciendo una serie de preguntas como estos:

1. ¿Se espera esta amenaza porque es una causa común de incidentes o porque
   ¿Son comunes las habilidades y los recursos necesarios para implementar la amenaza?
2. ¿El control deja el activo expuesto a esta amenaza de forma ocasional o parcial?
3. ¿No existen otras salvaguardas o condiciones entre el activo y la amenaza?
4. ¿La vulnerabilidad está presente de manera frecuente o constante?

Las organizaciones que usan una escala de probabilidad de 1 a 5 podrían derivar el puntaje de probabilidad reduciendo la puntuación máxima de '5' en '1' por cada respuesta 'sí' que brindan a la fortaleza preguntas Las organizaciones que usan una escala de probabilidad de 1 a 3 pueden optar por asignar .5 puntos por respuesta para llegar a puntajes entre 1 y 3.

Como ejemplo de este proceso de análisis, a una organización le preocupa que sus desarrolladores de software tener acceso al entorno de producción. El Control CIS 18.9 establece: "Mantener por separado entornos para sistemas de producción y no producción. Los desarrolladores no deberían tener acceso no supervisado a entornos de producción ". El modelo de amenaza que están evaluando se relaciona con promoción de código no seguro o que funciona mal al entorno de producción. La organización actualmente tiene una política que requiere la revisión y aprobación del código antes de promover el código para producción, pero muchos desarrolladores de software tienen acceso al entorno de producción en caso de que necesitan responder a emergencias.

Para estimar la probabilidad del riesgo, responden las preguntas de análisis de preparación de defensa abajo.

Tabla 84 - Ejemplo de análisis de preparación de defensa

Pregunta de análisis de preparación de defensa	Respuesta (1 = "Sí", 0 = "No")
¿Se espera esta amenaza porque es una causa común de incidentes, o porque las habilidades y recursos necesarios para promulgar la amenaza son comunes?	1

[21] http://binary.protect.io (consultado el 3 de enero de 2018)

[22] Si bien el análisis de riesgo binario proporciona un proceso analítico riguroso, debe modificarse para abordar los conceptos de "razonable" y "apropiado" que son centrales para el CIS RAM y los aspectos legales y

esfera reguladora.

140

Pregunta de análisis de preparación de defensa	Respuesta (1 = "Sí", 0 = "No")
¿El control deja el activo expuesto a esta amenaza? ocasionalmente o parcialmente?	1
¿No hay otras salvaguardas o condiciones entre el activo y la amenaza?	0 0
¿La vulnerabilidad está presente de forma frecuente o constante? ¿base?	1
Puntuación de probabilidad (suma de respuestas).	**4 4**

La organización llega a un puntaje de probabilidad de '4' después de su análisis. Si es descuidado o apurado el programador es la amenaza en este escenario, luego la organización responde con estos puntajes para Las siguientes razones.

1. La amenaza es una causa común de infracciones y requiere habilidades comunes para acceder a entorno de producción y código de promoción, por lo que la organización responde con '1'.
2. Las salvaguardas de acceso lógico que protegen el entorno de producción siempre permiten programadores para promover el código, por lo que la organización responde a esta pregunta con un '1'.
3. Porque los programadores generalmente se adhieren a políticas, prácticas de codificación seguras y flujos de trabajo documentados, existen otras salvaguardas que evitarían la promoción de Código dañino para el entorno de producción. Entonces la organización responde con un '0'.
4. Y la vulnerabilidad está constantemente presente, por lo que la organización responde nuevamente con un '1'.

Finalmente, agregan las respuestas para lograr su puntaje de probabilidad, que en este caso es '4'.

Las organizaciones deben ser conscientes de que el análisis de preparación para la defensa no es necesariamente evidencia basado, y no examina exhaustivamente todos los aspectos de la fuerza de control. El beneficio de El análisis de preparación para la defensa es para ayudar a las organizaciones de manera sistemática, cuidadosa y consistente estimar sus puntajes de probabilidad basados en criterios internos y externos.

Por ejemplo, una organización también puede analizar constantemente la preparación para la defensa preguntando preguntas similares a las siguientes:

1. ¿El activo en este escenario de amenaza es atractivo para los hackers con recursos suficientes?
2. ¿Es este ataque una causa común de infracciones en nuestra industria?
3. ¿Se ha evaluado este control como efectivo utilizando una prueba de penetración u otro riguroso ¿prueba?
4. ¿Es nuestro momento de detectar y prevenir el impacto de este ataque más corto que el tiempo del ataque? necesita crear un impacto?

La preparación para la defensa puede tener en cuenta la evidencia al revisar los datos de seguridad de la información sobre su entorno (si han implementado las herramientas necesarias para recopilar esa información), y al revisar las causas conocidas de eventos, incidentes e infracciones de seguridad de la información.

Uso de la probabilidad con el análisis de riesgos del deber de cuidado

Algunas organizaciones tienen fuentes de datos útiles para realizar análisis de probabilidad para ayudarlas Determinar la probabilidad de riesgos. El análisis de probabilidad requiere métodos estadísticos, bien perfeccionados habilidades de estimación y buenos datos para determinar la probabilidad de un evento o de eventos con cierta impactos.

Tabla 85 - Resumen de la evaluación del uso de la probabilidad con el análisis de riesgos del deber de cuidado

Beneficios	Límites
- Apoya la estimación basada en evidencia - Los evaluadores de riesgos pueden confiar en profesionales rigor para mejorar la estimación del riesgo a lo largo del tiempo	- Las estimaciones estadísticas deben abordar todos tipos de impacto para evaluar adecuadamente cada riesgo sobre la base del debido cuidado.

Esta sección propondrá un enfoque para vincular el análisis de probabilidad con las evaluaciones del "deber de cuidado", pero no presentará un método integral para hacerlo, ni proporcionará una explicación del Análisis de probabilidad al que se refiere esta sección. Lectores que usan análisis de probabilidad para Se alienta la gestión de seguridad de la información para explorar métodos de integración como esos descrito aquí.

El análisis de probabilidad es complementario a los métodos de evaluación de riesgos descritos en el CIS RAM, pero los lectores deben entender sus diferencias.

1. Con la orientación correcta, la aplicación de modelos de probabilidad a los riesgos individuales de ciberseguridad es (probablemente) más simple de lo que el lector pueda imaginar. [23]
2. La probabilidad se basa en la evidencia y puede ayudar a las organizaciones a modelar cada vez más realista escenarios de amenaza, especialmente a medida que aumenta el rigor de sus métodos.
3. La probabilidad se basa en décadas de metodología sólida, impulsada por profesionales estadísticos, que utilizan procesos universalmente reconocidos para reducir la incertidumbre. Las organizaciones que pueden usar métodos de probabilidad deberían hacerlo.
4. Los modelos de probabilidad a menudo resultan en rangos o curvas, en lugar de puntajes discretos como los producidos por la RAM. Los rangos de posibles resultados se asemejan mejor a la "estimación" que un valor discreto hace. Sin embargo, los rangos y las curvas son más difíciles de comparar. y priorizar que puntuaciones discretas.
5. Los escenarios de amenazas de ciberseguridad son variados y, por lo tanto, requieren una variedad de probabilidades métodos para estimar su probabilidad. Esto hace que sus resultados crudos sean difíciles de comparar y rango. Una simulación de Monte Carlo que proporciona un valor único (por ejemplo, una probabilidad de "22%" se robará una computadora portátil no encriptada) y un modelo Bayes que proporciona una curva que describe Varias posibilidades de probabilidad de impacto en dólares (como “13% de probabilidad de pérdida de $ 750,000 y 24% de probabilidad de pérdida de 177,000) no son fácilmente comparables. Y comparándolos con un El criterio de aceptación de riesgo único será igualmente difícil.
6. Los modelos de probabilidad por sí solos no se alinean naturalmente con las preguntas del deber de cuidado planteadas por reglamento o litigio. Las regulaciones y los litigios insisten en evaluar la "debida atención" por equilibrar diferentes tipos de cosas (seguridad de los clientes versus el valor de los servicios proporcionado a ellos, por ejemplo). Modelos estadísticos que describen el impacto en términos de uno (es decir, el costo de un impacto) se pierden otras consecuencias reales de las infracciones de seguridad cibernética, como daño a otros, o la carga de salvaguardas demasiado estrictas (es decir, reducción en servicios, riesgos para la seguridad del personal, dificultad para operar de manera rentable o los beneficios que un

[23] Douglas Hubbard de Hubbard Research ha publicado muchos libros sobre el tema, el último de que se centra exclusivamente en la ciberseguridad. Hubbard, Douglas y Richard Seierson. *Cómo Mida cualquier cosa en ciberseguridad.* Hoboken, Nueva Jersey: John Wiley & Sons, Inc., 2016.

organización proporciona a otros, etc.). Cuando todos los impactos se evalúan en términos de dólares,

Los jurados y jueces tienden a ver la evaluación de riesgos desfavorablemente. [24]

Pero las organizaciones que están bien capacitadas en estadística y estimación deberían usar modelos de probabilidad y simulaciones para alimentar su análisis del deber de cuidado. ¿Cómo, entonces, tal organización lograr esto usando el CIS RAM?

Dichas organizaciones "traducen" en frío el resultado de sus modelos de probabilidad (como Bayesian distribuciones, simulaciones de Monte Carlo o estimaciones) en los puntajes de probabilidad o puntajes de riesgo que se utilizan en el registro de riesgos.

Considere el caso de una distribución bayesiana por el riesgo de que el malware cause una violación en un extremo sistema de usuario, dado el uso de un sistema robusto de prevención de malware. La probabilidad de riesgo puede ser calculado como tal:

P (violación de malware | prevención de malware) = P (malware | prevención de malware) P (violación de malware | malware) + (1 - P (malware | prevención de malware) P (incumplimiento de malware | ~ malware) = (.05) (. 75) + (.95) (. 01) = 4.7%. [25]

Recuerde que la tabla de puntuación de impacto para una organización de Nivel 2 o Nivel 3 y Nivel 4 tiene cinco valores que describen niveles de previsibilidad. Una organización puede agregar fácilmente una columna a su tabla de definiciones de probabilidad (como en la Tabla 86) para indicar cómo asocian la previsibilidad con probabilidad.

Nota: Los valores de probabilidad proporcionados en la Tabla 86 son solo ilustrativos. Cada organización podría Determinar por sí mismos cómo asociar la previsibilidad con la probabilidad al definir su riesgo. criterios de evaluación. Con el tiempo, la organización debería revisar y actualizar esta tabla.

Tabla 86 - Ejemplos de definiciones de probabilidad alineadas con probabilidad

Probabilidad Puntuación	Previsibilidad	Probabilidad %
1	No previsible	<.5%
2	Previsible pero no esperado	<5%
3	Se espera que ocurra	<10%
4 4	Una ocurrencia común	<25%
5 5	Puede estar sucediendo ahora	<= 100%

La probabilidad de malware de la organización dado su robusto sistema de prevención de malware es del 4,7%, que está por debajo del 5% (la definición de la organización para la probabilidad de "previsible pero no esperado"). Esto los guía a seleccionar el valor de probabilidad de '2' para el riesgo de infección de malware. Lo harían luego seleccione los puntajes de impacto para tal escenario para derivar su puntaje de riesgo.

[24] Viscusi, W. Kip, “Jurados, jueces y maltrato de riesgos por parte de los tribunales”. *Journal of Legal Estudios* , vol. XXX (enero de 2001).

[25] Nota: El CIS RAM no espera que los lectores entiendan o usen análisis de probabilidad. Esta el cálculo se muestra solo para demostrar cómo se puede coordinar el análisis probabilístico con el CIS RAM.

Y debido a que algunos análisis de probabilidad dan como resultado múltiples posibilidades dentro de un rango (es decir, un 1% posibilidad de una falla completa del sistema, o una probabilidad del 15% de una falla parcial del sistema) un registro de riesgos simplemente puede mostrar el mismo riesgo dos veces, pero con dos evaluaciones de riesgo diferentes.

Resultados como estos (riesgos múltiples dentro de un rango) a menudo son causados por una condición previa que puede o no estar en su lugar cuando ocurre la amenaza. Por ejemplo, un bajo riesgo de un sistema completo la falla puede estar asociada con condiciones normales de operación, y un mayor riesgo puede estar asociado con una temporada alta u otra circunstancia no típica. Dos riesgos en el registro de riesgos podrían entonces describa los dos riesgos de manera diferente y mencione su dependencia de la condición previa (es decir, el riesgo uno es asociado con la temporada alta, el riesgo 2 está asociado con las operaciones normales).

Muchos modelos de probabilidad producen un rango de puntajes de probabilidad e impacto, como el Distribución bayesiana representada en la Figura 28.

Figura 28 - Ejemplo de curva de probabilidad

Un beneficio de dicho rango de probabilidad es que estima tanto la probabilidad como los valores de impacto de un riesgo. En su mayor probabilidad, parece haber una probabilidad de aproximadamente 24.9% de un impacto de $ 1MM. A su probabilidad más baja, parece haber menos del 1% de probabilidad de un costo de $ 20MM o más. Esta permite al cliente declarar una alta probabilidad de un costo menor o una probabilidad menor de un costo mayor costo. La organización podría modelar ambos escenarios para determinar cuál crea el mayor puntaje de riesgo para abordar ese riesgo.

Emparejando la curva de probabilidad con la tabla de definiciones de probabilidad modificada (Tabla 86), la más alta El puntaje de probabilidad (menos del 25%) parece estar en el borde superior de un puntaje de probabilidad de '4'.

Si la tabla de puntuación de impacto de la organización se refiere a los costos o el impacto del presupuesto (quizás en el Columna de objetivos) luego $ 1MM se consideraría dentro del contexto de esos valores de impacto. Por ejemplo, la organización puede determinar que una pérdida de $ 1MM llevaría más de un año recuperarse de, lo que indica un valor de impacto de '4' en su columna de Objetivos en la Tabla 87. Que

Page 144

los dejaría con un puntaje de riesgo de '16' al multiplicar el puntaje de probabilidad de '4' y el impacto puntaje de '4'.

Tabla 87 - Definiciones de impacto de ejemplo

Impacto Puntuación	Impacto a la misión	Impactar a Objetivos	Impacto a las obligaciones
	Misión: proporcionar información a ayudar a los pacientes remotos a permanecer saludable.	*Objetivos: operar rentable*	*Obligaciones: los pacientes no deben ser perjudicado por comprometido información.*
1	Los pacientes continúan accediendo información útil, y Los resultados van por buen camino.	Las ganancias están en el objetivo.	Los pacientes no experimentan pérdida de servicio o protección.
2	Algunos pacientes pueden no tener todo la información que necesitan como ellos lo solicitan.	Las ganancias están fuera del objetivo, pero están dentro varianza planificada	Los pacientes pueden estar preocupados, pero no perjudicado
3	Algunos pacientes no pueden acceder la información que necesitan	Las ganancias están apagadas varianza planificada y	Algunos pacientes pueden ser perjudicado financieramente o

	mantener buena salud resultados.	puede tomar un fiscal año para recuperarse.	reputacionalmente después compromiso de información o servicios.
4 4	Muchos pacientes constantemente no puede acceder beneficioso información.	Las ganancias pueden tomar más que un fiscal año para recuperarse.	Muchos pacientes pueden ser perjudicado financieramente o reputacionalmente
5 5	Ya no podemos proporcionar información útil para el control remoto pacientes	La organización no puede operar rentable	Algunos pacientes pueden ser perjudicado financieramente, reputacional o físicamente hasta e incluyendo la muerte.

Si bien las organizaciones pueden estar satisfechas con la facilidad con la que pueden alinear su probabilidad resultados a sus criterios de evaluación de riesgos de cuidado debido, la probabilidad debe ser modelada contra todos Criterios de impacto. El análisis de riesgos que solo considera los impactos financieros para la organización pierde un componente necesario del análisis de riesgos de ciberseguridad; estimar y asumir la responsabilidad de daño potencial que otros pueden sufrir. Además, la organización debe evaluar el riesgo de salvaguardas utilizando los mismos modelos de probabilidad.

Para obtener orientación exhaustiva y práctica sobre el uso del análisis de probabilidad para la decisión de seguridad cibernética: haciendo, consulte el libro, *Cómo medir cualquier cosa en ciberseguridad* de Douglas Hubbard. [26]

Observando cómo se puede detectar el riesgo realizado

Las evaluaciones de riesgos brindan a las organizaciones una idea de cómo los incidentes de seguridad y las infracciones previsiblemente ocurrirá. Esto brinda a las organizaciones la oportunidad de vincular su registro de riesgos a su procesos para la gestión de registros de seguridad y alertas, para la planificación de respuesta a incidentes y para formación en conciencia de seguridad. Todos estos beneficios se pueden agregar a un registro de riesgos agregando un solo columna "Riesgo realizado".

[26] Hubbard, Douglas W., Richard Seiersen. *Cómo medir cualquier cosa en ciberseguridad.* Hoboken NJ: John Wiley & Sons, Inc., 2016

Page 145

Esta columna, que podría seguir el modelo de amenaza en cualquiera de los registros de riesgos que se ilustran en este documento, describiría cómo la organización sabría si hubo un ataque o error progreso, o si ocurrió un incidente o evento.

Considere los siguientes riesgos:

Tabla 88 - Ejemplo de columna de riesgos realizados

Control actual	Vulnerabilidad	Amenaza	Riesgo realizado
Escaneos de vulnerabilidad ocurrir ocasionalmente y puede no identificar a todos sistemas que han sido en la red entre escaneos.	Sistemas que tienen se unió a la red entre esporádicos los escaneos no serán detectado	Hackers o malware puede atacar y controlar sistemas que no tienen ha sido detectado, controlado, y monitoreado	El tráfico IP se envía a o de los anfitriones cuyo MAC las direcciones no son en la vulnerabilidad salida de escaneo.
Escaneos de vulnerabilidad ocurrir cuando la información de amenaza El servicio anuncia un moderado a alto vulnerabilidad que necesita parches Equipo confiable sistemas de parches dentro 24 horas de anuncio.	Una ventana de 24 horas de la vulnerabilidad permanece con la corriente proceso.	Hackers o malware puede atacar y controlar sistemas que no tienen sido parcheado dentro el período de 24 horas después de la vulnerabilidad fue anunciado.	Tráfico inusual enviado a la sin parchar sistemas.
Escaneos de vulnerabilidad ocurrir cuando la información de amenaza	Empresa administración	Hackers o malware puede atacar y controlar	Comando SQL cadenas enviadas desde

El servicio anuncia un moderado a alto vulnerabilidad que necesita parches Parches del equipo la mayoría de los sistemas dentro de 24 horas de anuncio.	sistemas de aplicación están sin parchear por más de un año	empresa administración solicitud medio ambiente.	navegadores de clientes y de forma campos y URL peticiones.

La organización ahora tiene una manera simple de saber qué buscar en términos de eventos que se pueden registrar, para agregar indicadores de escalamiento a su documento del plan de respuesta a incidentes y para usar en la información capacitación en concientización de seguridad (especialmente para aquellos indicadores de riesgo realizados que son reconocibles por personal general).

Uso del riesgo realizado para el monitoreo: en el caso de la primera notación de “riesgo realizado”, el la organización puede decidir detectar riesgos comparando direcciones MAC en cachés ARP con las de su salida de escaneo de vulnerabilidad. Con las herramientas adecuadas o las habilidades de secuencias de comandos, esto puede ser simple de lograr para ellos.

Uso del riesgo realizado para la respuesta a incidentes: la organización puede tener en cuenta en su respuesta a incidentes planean que deben tomar medidas cuando aparece una dirección MAC para un dispositivo desconocido (que sería hipervigilante en este caso, pero para ilustrar el punto).

Uso de riesgo realizado para capacitación y sensibilización: y la organización puede usar esto como un oportunidad de describir a los ingenieros de sistemas y al personal de la mesa de ayuda información que pueda ayudar ellos detectan e investigan otras actividades inesperadas en la red.

Page 146

Aprovechamiento del análisis de riesgos del deber de cuidado para los modelos de madurez

Muchas organizaciones usan modelos de madurez para evaluar las capacidades de seguridad en su entorno. Las evaluaciones del modelo de madurez hacen preguntas sobre controles de seguridad específicos o grupos de control. Los evaluadores pueden determinar qué tan formalizado es el programa de seguridad de una organización. Modelos de madurez se puede alinear con las evaluaciones de riesgo de RAM de CIS alineando un control en el modelo de madurez con un control CIS correspondiente en un registro de riesgos para determinar la aceptabilidad del riesgo del vencimiento Puntuación.

Tabla 89 - Resumen de la evaluación del uso del análisis de riesgos del deber de cuidado para los modelos de madurez

Beneficios	Límites
- Las organizaciones pueden continuar evaluar la formalización de su programas de seguridad - Algunos puntajes de madurez moderados pueden ser suficiente si está alineado con razonable riesgos	- Algunas autoridades que insisten en evaluando organizaciones únicamente con modelos de madurez pueden no aceptar puntajes de madurez moderados que se alinean con riesgo razonable

Las evaluaciones del modelo de madurez generalmente piden a las organizaciones un conjunto de descripciones de control y proporcionan valores de opción múltiple como respuestas opcionales a la descripción del control. Por ejemplo, control Las descripciones para la gestión de vulnerabilidades pueden indicar algo similar a esto:

Las vulnerabilidades se resuelven en tres días hábiles.

Las respuestas opcionales serían similares a esto (aunque las respuestas varían de un modelo de madurez a el siguiente):

0 = no en su lugar

1 = ad hoc

2 = documentado

3 = aplicado consistentemente

4 = Probado y corregido
5 = Mejorado continuamente.

Si una organización aplica este proceso y comprueba el éxito con las pruebas semanales posteriores, pero no mejoran su prueba, responderían con un "4"

Si esta organización también realiza una evaluación de riesgo de RAM CIS, habrán examinado esto control en un formato de riesgo en su registro de riesgos. En este caso, habrían examinado el Control CIS 3.6 "Comparar análisis de vulnerabilidades consecutivos". Es posible que hayan determinado que la probabilidad y el impacto de las amenazas previsibles es aceptablemente bajo. Si su análisis de riesgos le dice a la organización que su proceso de revisión existente es aceptable en términos de riesgo, entonces también pueden notar que en su evaluación de madurez de esta manera.

Tabla 90 - Ejemplo de modelo de madurez asignado al riesgo

Controlar	Control existente	Puntuación de madurez	Riesgo Aceptación
Vulnerabilidades se resuelven	Escaneos semanales de vulnerabilidad revisar los hallazgos para determinar si alguna vulnerabilidad	4 4	Aceptar

Page 147

Controlar	Control existente	Puntuación de madurez	Riesgo Aceptación
dentro de tres días hábiles	fueron identificados en anteriores escaneos.		

Al alinear un puntaje de madurez con un puntaje de riesgo, la organización puede determinar si necesitan para, o desea, formalizar aún más el control. De esta manera, la organización puede continuar evaluando su programa de seguridad utilizando puntajes de madurez, pero no se siente obligado a mejorar continuamente a menos que exista una razón relacionada con el riesgo para hacerlo.

Técnicas de entrevista

Las entrevistas de evaluación de riesgos son momentos críticos para comprender y modelar el riesgo y deben ser abordado de manera diferente que para una evaluación de cumplimiento o una auditoría. En una evaluación de riesgos, los evaluadores preguntan sobre las salvaguardas existentes, como en una auditoría, pero en el contexto de lo previsible las amenazas pueden comprometer los activos de información dados esas salvaguardas.

Tabla 91 - Evaluación resumida de las técnicas de entrevista

Beneficios	Límites
- Aumenta la conciencia del riesgo entre entrevistados - Observa el conocimiento del personal clave de Problemas de riesgo.	- Descripciones de personal de salvaguardas y los riesgos pueden no ser precisos.

En una evaluación o auditoría de cumplimiento, el evaluador generalmente informa un "aprobado" o "fallido" o incluso un "Pase parcial" al observar si un control requerido está presente. Una puerta de cierre automático con un el bloqueo auditable puede ser "compatible" con un estándar de seguridad. Un firewall operativo puede calificar como "Pasar" para una auditoría del perímetro de la red. Cifrado entre un servidor de aplicaciones y un el servidor de la base de datos puede estar marcado como "verde" o "de bajo riesgo" en un informe. Pero en una evaluación de riesgos, el el evaluador de riesgos aporta conocimiento a la entrevista (y luego a la revisión de la configuración de control) que prueba de tensión las salvaguardas descritas.

Por ejemplo, ¿el conjunto de reglas del firewall no contiene más que las reglas y políticas mínimas que son necesarios para los negocios? Quién puede cambiar las políticas del firewall y cómo es su acceso rastreado? Quién tiene acceso a las interfaces CLI y webadmin del firewall, y desde qué redes? ¿La interfaz webadmin está activa? ¿Cómo se actualiza el firmware? ¿Cómo son los cortafuegos? registros de eventos revisados y analizados? ¿Se aplica el acceso a través de métodos de múltiples factores? Hace el ¿El cortafuegos falla abierto?

A medida que los encuestados brindan cada respuesta, el evaluador de riesgos debe considerar un correspondiente

amenaza para ayudarlos a modelar el riesgo. Puede ser apropiado modelar riesgos con el encuestado presente o después de la entrevista. Esto depende de una serie de factores, incluido el evaluador de riesgos consuelo en improvisar escenarios de amenazas para cada respuesta sobre una salvaguarda. Pero idealmente, el riesgo La entrevista de evaluación incluirá discusiones sobre amenazas para que las discusiones de riesgo total informen preguntas de seguimiento.

Considere cómo se desarrollarían las preguntas de la entrevista anterior cuando las respuestas de un entrevistado son emparejado con amenazas.

148 de 1189.

Tabla 92 - Emparejamientos de amenazas de la entrevista

Pregunta de entrevista	Respuesta	Amenaza pareada
¿El conjunto de reglas del firewall no contiene más que el reglas y políticas mínimas que son necesarios para los negocios?	No. Algunas políticas temporales aún puede estar funcionando	A los piratas informáticos les gusta explotar el firewall reglas que proporcionan acceso a Sistemas y servicios internos. ¿Cuáles son las posibilidades de que lo hagan? encontrar políticas permisivas en el cortafuegos ahora? (Nota: este es un excelente ejemplo de salvaguarda para observar más tarde).
¿Quién puede cambiar el políticas de firewall y cómo es su acceso rastreado?	Dos administradores tienen privilegios con unico cuentas Todos los cambios de firewall se registran y alertan a la equipo de seguridad.	Parece que dos administradores Ser un número bajo. Ellos compartir sus contraseñas con otros administradores para ayudar fuera cuando sea necesario?
Es la interfaz webadmin incluso activo?	Lo es, pero solo para uso interno redes	Los atacantes o el malware pueden intentar para iniciar sesión en el webadmin aplicación utilizando adivinado o Credenciales robadas. Cómo evitar que eso suceda?
¿Se aplica el acceso a través de métodos de múltiples factores?	Sí. Cada administrador usa una aplicación en su celular teléfono para recibir un fuera de banda, código de seis cifras que dura un minuto.	Podría una persona no autorizada acceder a su teléfono mientras está en un sistema que puede iniciar sesión en el interfaz webadmin con credenciales robadas?

Al responder a las respuestas con amenazas plausibles, el evaluador de riesgos puede generar un interés más interesante. entrevista sobre si un control está suficientemente diseñado y puede darles indicadores de qué salvaguardas y configuraciones que les gustaría seguir durante la configuración posterior comentarios

Además de combinar las respuestas de los entrevistados con amenazas plausibles, las organizaciones deben planificar sus discusiones de evaluación de riesgos en la línea de una estructura o conversación planificada. Esto ayuda Asegurarse de que el evaluador de riesgos aborde un conjunto de temas que deben entenderse durante un riesgo evaluación, y les permite confiar en un plan en lugar de agotarse con constante improvisación.

Considere usar una o más de estas rúbricas para establecer el ritmo de las entrevistas de evaluación de riesgos.

Rúbrica 1: "Ciclo de vida completo de uso" o "Auditoría de procesos". Este método obliga a la evaluación de riesgos los participantes piensen en los activos de información como algo que cambia en el transcurso de su uso. El proceso generalmente es útil para los evaluadores que tienen experiencia en operaciones de seguridad, porque les exige tener un conocimiento práctico de cómo se desarrollan los activos de información y gestionado

Un ejemplo de un proceso de entrevista de ciclo de vida completo de uso ilustrará el punto.

1. El ciclo de vida de un activo de información comienza con la definición de los requisitos comerciales que es

siendo construido para.
2. Luego se enumerarán las especificaciones técnicas para preparar el activo de información para satisfacer el requisitos comerciales
3. Luego se seleccionaría un estándar de endurecimiento para construir el activo desde

Page 149

4. El activo de información se crea, instala o implementa con derechos de acceso primarios.
5. Se establecen más derechos de acceso y el activo de información si está configurado.
6. El activo de información se incluye en procesos de seguridad comunes, como el registro gestión, gestión de vulnerabilidades, gestión de cambios, pruebas de penetración y parches de gestión de horarios y rutinas.
7. Y finalmente, termina su ciclo de vida al ser desmantelado, perdido, robado o dañado.

El ciclo de vida de un activo de información proporciona a un evaluador de riesgos indicaciones de si y cómo Se aplican salvaguardas al activo de información.

Entonces, si las preguntas iniciales de la entrevista determinan que no existe un proceso riguroso para identificar negocios requisitos o especificaciones técnicas para implementaciones de servidores, luego salvaguardas que serán discutido más adelante, como la gestión de registros y la gestión de cambios, se evaluará con el conocimiento de que los requisitos iniciales para el servidor no se conocen de manera confiable. El endurecimiento de un servidor y los procesos de configuración pueden permitir demasiados servicios y privilegios de acceso porque Los requisitos comerciales y las especificaciones técnicas son las etapas apropiadas para determinar menos capacidades y menos privilegios para un servidor.

Para el momento en que el evaluador de riesgos llegue a preguntas relacionadas con la gestión de registros, también saber preguntar, "¿Cómo sabes que los registros del servidor son apropiados para los riesgos y la función de el sistema? "Para la gestión de vulnerabilidades, el evaluador de riesgos podría preguntar:" ¿Cómo sabe el diferencia entre un servicio de vulnerabilidad que es apropiado para el negocio y uno que no lo es? ”Y "¿Cómo prueba parches, actualizaciones y cambios de configuración si no sabe qué ¿Servicios críticos para el negocio que puede interrumpir?

Nuevamente, este proceso es apropiado para profesionales de seguridad experimentados, o individuos que tienen experiencia en operaciones técnicas y comprender cómo las etapas anteriores de un activo de información El ciclo de vida puede influir en la efectividad de las salvaguardas en etapas posteriores.

Rúbrica 2: "Ciclo de vida de gestión de seguridad" El ciclo de vida de gestión de seguridad de una información el activo se asemeja a las evaluaciones del modelo de madurez utilizadas en otros métodos de evaluación de seguridad. por aquellos que no están familiarizados con los modelos de madurez, se parecen a algo similar a la tabla a continuación.

Tabla 93 - Ejemplo de modelo de madurez

Nivel de madurez	Descripción
1 - Ad hoc	No es consistente en la práctica.
2 - Documentado	Documenta los requisitos del estado para procesos y configuraciones.
3 - Implementado	Los requisitos se aplican a los activos de información como salvaguardas.
4 - Evidenciado	Las pruebas demuestran que las salvaguardas son efectivas.
5 - Detect & Correct Management	detecta cuando ocurren fallas y mejora las fallas identificadas.

Muchas evaluaciones imponen modelos de madurez como el que se muestra arriba. En estos evaluaciones, los evaluadores a menudo confían en la selección de un puntaje de madurez como su descripción total de una salvaguardia. Pero sin una comprensión de la resistencia de un activo de información a lo previsible Amenazas, la aceptabilidad de un control será difícil de evaluar.

A pesar de esta debilidad, un modelo de madurez puede ser útil para evaluar el riesgo. Por ejemplo, mientras que un El evaluador de riesgos está evaluando un control para determinar su resistencia frente a las amenazas, podrían utilizar el modelo de madurez para comprender la probabilidad de riesgo actual y futuro.

Un ejemplo de conversación de evaluación de riesgos sobre el endurecimiento del servidor demuestra este proceso abajo.

Page 150

Asesor (haciendo la pregunta “1 - Ad hoc”) : ¿endurece sus servidores a un bien conocido?
¿estándar?

Ingeniero de sistemas : Sí, nuestros servidores se implementan utilizando imágenes basadas en políticas SCAP que
Admite cada versión del sistema operativo.

Asesor (Haciendo la pregunta "2 - Documentada") : ¿Cómo saber qué políticas SCAP debe
aplicar a cada servidor?

Ingeniero de Sistemas : Tenemos estándares que enumeran cada sistema operativo implementado y
versión, y que indican la versión de la política SCAP que se utilizará para cada sistema operativo.

Asesor (Haciendo la pregunta “3 - Implementada”) : ¿Cuántos servidores en producción hay ahora?
basado en las políticas SCAP?

Ingeniero de sistemas : todos los servidores se crearon en el último año, por lo que todos están configurados con su
política SCAP coincidente como su línea de base.

Asesor (Haciendo la pregunta "4 - Evidenciada") : ¿Todavía están configurados para el endurecimiento?
estándar con el que comenzaron?

Ingeniero de Sistemas : Creo que sí. Algunas configuraciones deben haber cambiado para nuevos requisitos o
solución de problemas. A veces hacemos cambios temporales que no siempre cambiamos.

Asesor (Haciendo la pregunta “5 - Detectar y corregir”) : ¿Cómo saber cuándo un servidor no funciona?
¿Ya está configurado para coincidir con su política SCAP?

Ingeniero de sistemas : las evaluaciones de vulnerabilidad muestran cuándo hay vulnerabilidades, así que esa es una
camino. Pero no estamos verificando estrictamente el cumplimiento de la política SCAP después de los servidores
han sido desplegados

Ahora la organización sabe que comenzaron a configurar servidores de forma segura, pero que el
los servidores comienzan a divergir de su configuración segura conocida y la organización puede no
detectarlo para corregirlo, a menos que el software de exploración de vulnerabilidades compare las configuraciones del servidor con
sus políticas SCAP.

Los métodos de entrevista de evaluación de riesgos pueden ayudar a impulsar el descubrimiento y el análisis de muchas maneras, y
Ningún método individual es ideal. Las organizaciones deberían considerar intentar una variedad de métodos para ver
que funcionan mejor en diferentes escenarios. Pero si hay una regla para aplicar en el desarrollo de una entrevista
estilo es este: Sea flexible con el medio ambiente, la capacidad de los participantes y asesores, y
La naturaleza de la información que está tratando de obtener. Seguir con un método a lo largo de un
la evaluación perderá oportunidades para descubrir riesgos.

Evaluación de riesgo inherente

Algunas organizaciones están interesadas en comprender el "riesgo inherente" de un alcance de información
bienes. El “riesgo inherente” se define en el Glosario como “La probabilidad de un impacto cuando una amenaza
compromete un activo desprotegido ". Un registro de riesgos que evalúa el" riesgo inherente "sería casi
idéntico a las plantillas proporcionadas en el *CIS_RAM_Workbook* pero no tomaría en cuenta ni consideraría
controles establecidos para proteger los activos de información.

Las organizaciones que buscan riesgos inherentes a menudo desean determinar cosas como:

1. ¿Qué pasivos potenciales enfrentamos en la empresa A frente a la empresa B?
2. Si trasladamos un proceso de negocio a un servicio en la nube, ¿cuál es el riesgo / recompensa de la opción A?
   ¿Cuál usa todos nuestros datos, en comparación con la Opción B con algunos de nuestros datos?
3. Si involucramos este proceso de negocio / tecnología / instalación, ¿qué nuevas regulaciones
   requisitos vamos a soportar?
4. ¿Cuál es el beneficio actual de nuestro programa de seguridad existente?

Page 151

Y aunque el análisis de riesgo inherente puede proporcionar respuestas rápidas a estas preguntas, parece que plantean un estado ficticio para la mayoría de las situaciones. Parecen imaginar entornos en los que hay Realmente no hay controles de seguridad. Un análisis rápido puede describir los beneficios y los límites del riesgo inherente. análisis en la Tabla 93.

Tabla 94 - Evaluación resumida de la evaluación del riesgo inherente

Beneficios	Límites
- Se alinea con alguna evaluación de seguridad estándares, como el FFIEC Herramienta de evaluación de ciberseguridad. - Proporciona una base para una estimación rápida de pasivos potenciales de ciertos emprendimientos o arquitectura técnica decisiones - Puede ayudar a crear conciencia entre los no gestión técnica de la necesidad de continuar invirtiendo en información programas de seguridad, salvaguardas y conciencia.	- Asume una condición ficticia sin controles. - No evalúa el potencial cargas (ya sean bajas o altas) de salvaguardas en propuestas comerciales, que sean materiales para el atractivo de la proposición.

Si los evaluadores de riesgo tienen la intención de agregar un análisis de riesgo inherente a sus registros de riesgo, pueden hacerlo en las plantillas proporcionadas en el *CIS_RAM_Workbook* agregando columnas a la izquierda de lo observado columnas de riesgo. El registro de riesgos podría comparar el potencial de pleno e inmediato. compromiso de los activos con el estado actual de los controles y el estado propuesto de los controles. Las organizaciones primero deben determinar qué valor proporciona este análisis.

Análisis de causa raíz

Porque las organizaciones identificarán las debilidades en las salvaguardas y propondrán riesgos tratamientos para abordar esos riesgos, deberán comprender la causa real de la vulnerabilidades para garantizar que las vulnerabilidades no vuelvan a ocurrir. Este proceso de identificación del Las causas subyacentes de debilidades o fallas se denominan "análisis de causa raíz".

Tabla 95 - Evaluación resumida del análisis de causa raíz

Beneficios	Límites
- Ayuda a la organización a reducir probabilidad de recurrencia de la debilidad. - Ayuda a la organización simultáneamente abordar otras debilidades que pueden resultado de la causa raíz.	- Puede ser difícil identificar la raíz real porque la organización comienza a usar el proceso. - El análisis de causa raíz puede conducir a uno causa raíz cuando otras causas raíz pueden ser extrañado

Una práctica generalmente aceptada para identificar las causas fundamentales es realizar un ejercicio de "cinco porqués". Esto implica que el evaluador de riesgos identifique de forma recurrente la razón subyacente de un problema y el causas del problema, hasta que se identifique una "causa raíz" del problema.

El análisis de causa raíz es similar al diagrama a continuación.

Página 152

Figura 29 - Modelo de análisis de causa raíz

Si bien el análisis de la causa raíz se realiza clásicamente preguntando "por qué" cinco veces más profundamente descubra la causa raíz de un problema, este ejemplo llegó a una causa raíz plausible después de preguntar "Por qué" cuatro veces. Esto se debe a que una organización puede descubrir la causa raíz con más o menos preguntas de cinco.

En este caso, el evaluador de riesgos habrá notado que una página web es vulnerable a una inyección SQL ataque. Si su tratamiento de riesgo recomendado fue simplemente, "filtre todos los objetos de formulario en la página para para evitar caracteres especiales, los desarrolladores de la aplicación corregirían el error identificado y luego probablemente repita el error la próxima vez que tuvieron un cambio de emergencia en la aplicación.

Sin embargo, después de este análisis de causa raíz, la organización sabe abordar ambos debilidad (la entrada no filtrada en la página de la aplicación) y la causa raíz (la falta de seguridad codificación durante o inmediatamente después de cambios de emergencia).

El análisis de causa raíz debe ser parte de todas las evaluaciones de vulnerabilidad, ya sea que ocurran durante un evaluación de riesgos, una auditoría o después de un incidente de seguridad a medida que la gerencia determina las lecciones aprendido.

Page 153

Recursos útiles

CIS (Centro de seguridad de Internet)
CIS (Center for Internet Security, Inc.) es una entidad sin ánimo de lucro y con visión de futuro que aprovecha el poder de una comunidad global de TI para salvaguardar las organizaciones privadas y públicas contra el ciber amenazas Nuestros CIS Controls ™ y CIS Benchmarks ™ son el estándar global y mejor reconocido prácticas para proteger los sistemas y datos de TI contra los ataques más generalizados. Estos probados las pautas son continuamente refinadas y verificadas por un voluntario, comunidad global de experimentados Profesionales de TI. CIS es el hogar del Centro de análisis e intercambio de información multiestatal (MS-ISAC®), el recurso de referencia para la prevención, protección, respuesta y recuperación de amenazas cibernéticas para Entidades gubernamentales estatales, locales, tribales y territoriales de EE. UU. (www.cisecurity.org)

Laboratorios de seguridad HALOCK
Establecida en 1996, HALOCK Security Labs es una empresa de servicios profesionales de seguridad de la información. con sede en Schaumburg, IL. Por más de 20 años, HALOCK ha brindado Seguridad Impulsada por Propósito

servicios para ayudar a las organizaciones a lograr su misión y objetivos a través de una seguridad sólida prácticas HALOCK utiliza sus profundos antecedentes en el panorama legal y regulatorio, seguridad tecnologías y estándares, gobierno empresarial y análisis de datos para proporcionar datos basados en evidencia Análisis de seguridad y orientación a sus clientes. (www.halock.com)

Para orientación en la implementación de la RAM CIS: (www.halock.com/cisram)

Consejo DoCRA
El Consejo DoCRA mantiene y educa a los profesionales de riesgo sobre el uso del deber de cuidado Estándar de análisis de riesgos (DoCRA) en el que se basa CIS RAM. Si bien DoCRA es aplicable a evaluación del riesgo de seguridad de la información, está diseñado para ser generalmente aplicable a otras áreas de negocio que debe gestionar el riesgo y el cumplimiento normativo. (www.docra.org)

Organización Internacional de Normalización (ISO ®)
ISO proporciona a los profesionales de seguridad de la información un conjunto de estándares y certificaciones para gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información ("SGSI"). ISO 27001 es un método basado en el riesgo para que las organizaciones aseguren los activos de información para que puedan respaldar el contexto comercial y los requisitos de las partes interesadas. ISO 27005 es una información proceso de evaluación de riesgos de seguridad que se alinea con CIS RAM. (https://www.iso.org/isoiec-27001-información-seguridad.html)

Instituto Nacional de Estándares y Tecnología (NIST)
NIST proporciona una serie de estándares y recomendaciones para asegurar sistemas e información, conocido como "Publicaciones especiales" en la serie SP 800. NIST SP 800-30 proporciona orientación para evaluando el riesgo de seguridad de la información, NIST SP 800-37 y NIST SP 800-39, cada uno presente enfoques para gestionar el riesgo de seguridad de la información dentro de una organización. Mientras estos los enfoques están diseñados para abordar los sistemas de información federales y los roles de referencia dentro de agencias federales, sus principios y prácticas son generalmente aplicables a muchas organizaciones. (https://csrc.nist.gov/publications/sp)

NIST también proporciona el Marco para mejorar la infraestructura crítica ("Ciberseguridad Marco de referencia"). El marco organiza controles de seguridad de la información dentro de una estructura que se prepara y responde a incidentes de seguridad cibernética. El Marco de Ciberseguridad alinea su categorías y subcategorías de controles con los de otros documentos de control, incluidos los Controles CIS. (https://www.nist.gov/framework)

Page 154

Asociación de Auditoría y Control de Sistemas de Información (ISACA ®)
Conocido por sus estándares y certificaciones de garantía de TI, ISACA proporciona una información marco de gestión de riesgos de seguridad conocido como Risk IT. Risk IT basa su método de análisis de riesgos en ISO 31000, y agrega gobierno de riesgos y respuesta al análisis para proporcionar un ciclo de vida de TI gestión de riesgos. (http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management / Pages / default.aspx)

Análisis de riesgo binario (BRA)
Binary Risk Analysis se publica como versión 1.0. El método de análisis se presenta como hoja de trabajo y una aplicación en el sitio web de alojamiento. BRA proporciona a los analistas de riesgos un proceso conciso y consistente para evaluar los riesgos de seguridad de la información desglosando el componentes de un escenario de amenaza, incluidas las capacidades de defensa contra robustez variable y amenazas comunes (http://binary.protect.io)

Instituto justo
Fair Institute mantiene y educa a analistas de riesgos sobre el uso del Análisis Factorial de Información Riesgo. El método FAIR es similar al BRA en que proporciona un método consistente para evaluar riesgo de información basado en las características de los componentes de riesgos de información. https://www.fairinstitute.org/

Todas las referencias a herramientas u otros productos en este documento se proporcionan solo con fines informativos, y no representan el respaldo por parte de CIS de ninguna compañía, producto o tecnología en particular.

Información del contacto

CEI
31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
controlesinfo@cisecurity.org

Laboratorios de seguridad HALOCK
1834 Walden Office Sq. Ste 200
Schaumburg, IL 60173
847.221.0200
cisram@halock.com