PUESTA EN PRÁCTICA DE LA PLANTILLA DE GESTIÓN DE RIESGOS DE LA CADENA DE SUMINISTRO DE PROVEEDORES PARA PEQUEÑAS Y MEDIANAS EMPRESAS

Septiembre de 2021

Esta página se dejó intencionalmente en blanco.

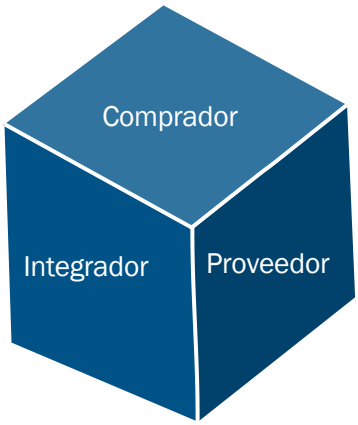
PUESTA EN PRÁCTICA DE LA PLANTILLA DE GESTIÓN DE RIESGOS DE LA CADENA DE SUMINISTRO DE PROVEEDORES PARA PEQUEÑAS Y MEDIANAS EMPRESAS

Resumen ejecutivo

Las 31.7 millones de pequeñas y medianas empresas (SMB, por sus siglas en inglés) de los Estados Unidos representan el 41.7 por ciento de los empleados del sector privado y casi la mitad del producto interno bruto del país.[i] El Equipo Operativo (Equipo Operativo) de Gestión de Riesgos de la Cadena de Suministro de Tecnologías de la Información y las Comunicaciones (ICT SCRM, por sus siglas en inglés) estableció un grupo de trabajo para SMB (Grupo de Trabajo) con el propósito de centrarse en las necesidades específicas de la cadena de suministro de ICT de las SMB de tecnologías de la información (IT, por sus siglas en inglés) y comunicaciones. A los fines de este informe, las pequeñas y medianas empresas de IT o comunicaciones se definen como "organizaciones con hasta 500 empleados, aunque se prevé que la mayoría de estas organizaciones tengan menos de 100 empleados".[ii]

El Grupo de Trabajo identificó casos de uso que suelen encontrar los proveedores de IT y comunicaciones pequeños y medianos, para lo cual utilizó la Plantilla de Gestión de Riesgos de la Cadena de Suministro de Proveedores (SCRM) de ICT ("Plantilla de Proveedores").[iii] Esta plantilla incluye preguntas estandarizadas destinadas a comunicar la postura con respecto a los riesgos de la cadena de suministro de ICT desde la perspectiva del comprador, el integrador y el proveedor, con el fin de lograr mejores resultados, como se muestra en la figura 1.

Figura 1: Tres roles que asumen las pequeñas y medianas empresas



- Comprador: propietario, operador o directivo de una SMB que desea realizar una compra en la que la seguridad de la cadena de suministro de ICT es motivo de preocupación.
- Integrador: un integrador de SMB adquiere e implementa productos o servicios de ICT en nombre de sus clientes.
- Proveedor: propietario, operador o directivo de una SMB que desea obtener un contrato en el que la seguridad de la cadena de suministro de ICT es motivo de preocupación para el potencial cliente.

[i] https://cdn.advocacy.sba.gov/wp-content/uploads/2020/11/05122043/Small-Business-FAQ-2020.pdf
[ii] *Definiciones para pequeñas y medianas empresas.* (2021). Washington, DC: Consejo de Coordinación del Sector de IT (IT Sector Coordinating Council)
[iii] https://www.cisa.gov/publication/ict-scrm-task-force-vendor-template

El Grupo de Trabajo analizó la Plantilla de Proveedor desde la perspectiva de una SMB de IT o comunicaciones, seleccionó una o más perspectivas descritas anteriormente como aplicables a cada uno de los casos de uso identificados y documentó los beneficios y resultados deseados para el caso de uso de cada perspectiva seleccionada. Luego, el Grupo de Trabajo seleccionó, **textualmente** de la Plantilla de Proveedores, aquellas preguntas que eran **más relevantes e importantes** para los casos de uso **con respecto a las SMB de IT y comunicaciones.** Si una SMB utiliza varios casos de uso, puede ser útil identificar preguntas comunes entre ellos. Las respuestas a las preguntas podrían estar entre "sí" y "no". Como resultado, el Apéndice B incluye una lista de recursos que las SMB pueden utilizar para identificar métodos que permitan aumentar la seguridad de su cadena de suministro. El Apéndice C, incorporado como referencia, es una hoja de cálculo adjunta que contiene las mismas preguntas seleccionadas en cada caso de uso y presentadas en un formato alternativo.

OBJETIVO:

Este producto ayuda a mitigar los riesgos de la cadena de suministro de ICT, con un enfoque específico en hacer que la Plantilla de Proveedores de la empresa sea más accesible y fácil de utilizar para las SMB.

ALCANCE:

El Grupo de Trabajo seleccionó tres casos de uso comunes que ayudarán a identificar los riesgos de la cadena de suministro, como las amenazas y vulnerabilidades relacionadas con la Base de Datos Nacional de Vulnerabilidades (National Vulnerability Database).[iv] El Grupo de Trabajo de Evaluación de Amenazas del Equipo Operativo de SCRM de ICT publicó una lista extensa de escenarios de amenazas y posibles mitigaciones para esas amenazas.[v] Si bien es importante que las empresas consideren todas las amenazas a su cadena de suministro, los recursos limitados exigen evaluar y priorizar las amenazas que representan el mayor riesgo y las posibles consecuencias. Una vez que una organización mitiga las amenazas identificadas de la mejor manera posible, debe considerar amenazas adicionales de forma continua.

METODOLOGÍA:

El Grupo de Trabajo identificó varios escenarios de casos de uso y los redujo a los tres casos de uso incluidos en este informe como punto de partida. Cada caso de uso identificó preguntas específicas de la Plantilla de Proveedores y describió qué preguntas pertenecían al rol de comprador, integrador o proveedor.

[iv] https://nvd.nist.gov/
[v] https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v2.pdf

Índice

Cifras

GRUPO DE TRABAJO PARA PEQUEÑAS Y MEDIANAS EMPRESAS (SMB)

Agradecemos al Grupo de Trabajo y a todo el Equipo Operativo por su participación, y hacemos un agradecimiento especial a las personas mencionadas a continuación que participaron en los Equipos de Redacción:

Equipo directivo:

	Nombre	Organización
Copresidente	Ola Sage	CyberRx
Copresidente	Robert Arnold	DHS CISA
Copresidente	Tamber Ray	NTCA - The Rural Broadband Association

Participantes del Equipo de Redacción:

Nombre	Organización
Andras Szakal	The Open Group
Chad Kliewer	Pioneer
Frank Bulk	Premier Communications
Jack Nemceff, Valerie Dumas	Departamento de Estado (Dept. of State)
Jeffery Goldthorp, Zenji Nakazawa	Comisión Federal de Comunicaciones (Federal Communications Commission)
Jerry Horton	Blue Valley Inc.
John Minasyan	Belkin International
Kathryn Basinsky, Megan Doscher	Administración Nacional de Telecomunicaciones e Información (National Telecommunications and Information Administration)
Rebecca Adams, Jennifer Hunt, Briana Alston	DHS CISA

CASO DE USO 1

APLICACIÓN DE LA GESTIÓN DE RIESGOS DE LA CADENA DE SUMINISTRO DE PROVEEDORES DE ICT A LOS CONTROLES DE ACCESO FÍSICO Y LÓGICO

Descripción

Se presentan riesgos cada vez que una pequeña o mediana empresa (SMB) otorga acceso físico o lógico a instalaciones o sistemas como condición de un contrato o del aprovisionamiento, el mantenimiento o el soporte de un producto o servicio. Las SMB deben abordar dichos riesgos antes de otorgar acceso. A modo de ejemplo, el acceso puede implicar lo siguiente:

1. Acceso a ubicaciones físicas que albergan controles industriales críticos o sistemas de infraestructura de edificios (por ejemplo, ventilación y aire acondicionado [HVAC, por sus siglas en inglés], agua, energía, equipos de telecomunicaciones o delimitación, seguridad perimetral, videovigilancia, detección de movimiento) o infraestructura de tecnología de la información o sistemas de información (IT/IS, por sus siglas en inglés) críticos (por ejemplo, enrutadores y conmutadores, servidores, sistemas de seguridad de IT/IS).

2. Acceso lógico a cualquier sistema, incluidos, entre otros, los enumerados anteriormente, como el acceso por tiempo limitado o la conectividad remota persistente.

Estos se ofrecen a modo de ejemplo, y no pretenden ser exhaustivos. El acceso puede tener un límite de tiempo, según los requisitos del proyecto, o puede ser continuo para proporcionar mantenimiento y soporte ininterrumpidos. Independientemente del tipo o la duración del acceso requerido, existen los mismos riesgos y las SMB deben abordarlos.

¿QUÉ RESULTADOS DE DECISIONES RESPALDAN LAS PREGUNTAS?

1. ¿Debemos conceder o aceptar el acceso?
    a. Identificación: ¿Mi SMB cuenta con protecciones adecuadas si se otorga acceso a instalaciones o sistemas?
    b. Protección: ¿Mi SMB cuenta con suficiente seguridad de personal, acceso físico y controles de acceso lógico para proteger mi negocio?
    c. Detección: ¿Mi SMB tiene un monitoreo adecuado para detectar cuando el acceso a instalaciones o sistemas no está autorizado?
    d. Respuesta: ¿Mi SMB tiene suficiente capacidad para responder ante el acceso no autorizado? ¿A quién se debería notificar en caso de infracción?
    e. Recuperación: ¿Mi SMB tiene planes de contingencia establecidos en caso de que ocurra un evento disruptivo debido al acceso no autorizado a las instalaciones o sistemas?
2. Debida diligencia: ¿El proveedor tiene evidencia para demostrar lo siguiente?
    a. Existen políticas y procedimientos establecidos para lo siguiente:
        i. Examinar o evaluar al personal en función de su necesidad de acceso y el acceso del personal está limitado únicamente a las áreas necesarias para cumplir con su función específica.
        ii. Gestionar el control de acceso físico a instalaciones con activos cibernéticos (dispositivos de red, instalaciones de datos, paneles de conexión, sistemas de control industrial, lógica programable, etc.).
        iii. Supervisar las autorizaciones del personal independiente y detectar accesos no autorizados.

b. Los incidentes de seguridad física y los eventos sospechosos se elevan al personal de operaciones de ciberseguridad.

c. ¿Se proporciona capacitación de concientización sobre seguridad para el acceso lógico? Se proporciona protección contra amenazas de agentes internos para la información de identificación personal (PII, por sus siglas en inglés) de los clientes de SMB.

Resultado de la decisión del comprador

La SMB tiene la tranquilidad de que el proveedor de servicios gestionados (MSP, por sus siglas en inglés) comparte su priorización de la seguridad de la cadena de suministro como condición para la adjudicación.

Resultado de la decisión del integrador

La SMB obtiene una mejor comprensión del perfil de riesgo del MSP, lo que puede utilizarse como herramienta para evaluar a otros proveedores.

Resultado de la decisión del proveedor

La SMB puede demostrar que el aspecto de gestión de riesgos del negocio se examinó correctamente.

Beneficios como comprador, integrador o proveedor

La aplicación de esta plantilla ofrecerá muchos beneficios, por ejemplo, los siguientes:

1. Ayudar a las SMB a evaluar áreas potenciales de riesgos al agregar o modificar cualquier producto o servicio a su entorno.
2. Ayudar a las SMB a desarrollar políticas, procedimientos y mitigaciones para abordar la postura con respecto a los riesgos presentada por la adición o la modificación de productos o servicios que requieren acceso de terceros.
3. Proporcionar indicadores de desempeño a las SMB y a los proveedores potenciales para medir los acuerdos de nivel de servicio o negociar acuerdos contractuales.
4. Construir una matriz de decisiones para la SMB con respecto a la creación de solicitudes de propuestas y selección de productos y servicios.
5. Proporcionar a la SMB una metodología para lograr el cumplimiento normativo o industrial, por ejemplo: Estándar de Seguridad de Datos del Sector de Tarjetas de Pago (PCI/DSS, por sus siglas en inglés), ISO 27001, NIST 800-53, etc.

REFERENCIAS DE LAS PLANTILLAS DE PROVEEDORES (COMPRADOR, INTEGRADOR, PROVEEDOR)

Para ayudar a su organización, las siguientes preguntas se aplican a la mayoría de las SMB y a todos los roles de la cadena de suministro: comprador, integrador o proveedor. Estos no pretenden ser exhaustivos; más bien, son representativos de las prácticas básicas de gestión de riesgos de la cadena de suministro. La Plantilla de Proveedores completa está disponible en https://www.cisa.gov/publication/ict-scrm-task-force-vendor-template.

Preguntas iniciales

Si puede proporcionar respuestas afirmativas a las siguientes preguntas Y documentación de respaldo vigente, puede omitir TODAS las preguntas restantes.

Si una SMB utiliza varios casos de uso, puede ser útil identificar preguntas comunes entre ellos. Las respuestas a las preguntas podrían estar entre "sí" y "no".

1.1 ¿Ha proporcionado previamente información sobre gestión de riesgos de la cadena de suministro a esta organización?

Si responde "Sí", proporcione una revisión actualizada que cubra los cambios materiales.

O BIEN

1.2 ¿Tiene controles completamente alineados con NIST SP 800-161, Prácticas de gestión de riesgos de la cadena de suministro para los sistemas y organización de información federales?

Si respondió afirmativamente a ALGUNA de las preguntas anteriores, puede adjuntar documentación de respaldo y omitir las preguntas restantes.

Seguridad en el diseño y la ingeniería

3.17 ¿Su organización analiza las vulnerabilidades para identificar la causa raíz?

Seguridad de la información

4.3 ¿Tiene implementadas políticas de seguridad de la información que cubran las políticas de privacidad y estén disponibles públicamente para toda la empresa?

4.7 ¿Tiene un programa de gestión de activos que se mantenga regularmente y esté aprobado por la gerencia para sus activos de IT?

4.10 ¿Tiene políticas y prácticas documentadas de hardware y software para garantizar la integridad de los activos?

4.15 ¿Tiene políticas y procedimientos de control de acceso a la red implementados para sus sistemas de información que estén alineados con los estándares de la industria o los marcos de control?

4.16 ¿Se necesita capacitación en ciberseguridad para el personal que tiene derechos administrativos sobre los recursos informáticos de su empresa?

4.17 ¿Incluye obligaciones contractuales para proteger la información y los sistemas de información que manejan sus proveedores?

4.19 ¿Su organización cuenta con estándares de fortalecimiento para los dispositivos de red (por ejemplo, puntos de acceso inalámbricos, firewalls, etc.)?

4.21 ¿Tiene prácticas de detección de incidentes definidas y documentadas?

4.25 ¿Tiene un proceso de respuesta a incidentes documentado y un equipo de respuesta a incidentes especializado?

4.26 ¿Tiene procesos o procedimientos para recuperar la funcionalidad completa, incluida la verificación de integridad, después de un incidente importante de ciberseguridad?

Seguridad física

5.2 ¿Tiene políticas y procedimientos de seguridad documentados que aborden el control de acceso físico a activos cibernéticos (dispositivos de red, instalaciones de datos, paneles de conexión, sistemas de control industrial, lógica programable, etc.)?

5.3 ¿Tiene políticas documentadas que aborden la capacitación del personal, lo que incluye procedimientos para limitar el acceso físico a activos cibernéticos (dispositivos de red, instalaciones de datos, paneles de conexión, sistemas de control industrial, lógica programable, etc.) a solo aquellas personas que tengan una necesidad demostrada?

5.4 ¿Tiene un proceso documentado de respuesta a incidentes de seguridad para abordar incidentes de seguridad física potenciales o presuntos (por ejemplo, posible acceso de intrusos, equipos faltantes, etc.)?

5.6 ¿Existen mecanismos de cumplimiento (por ejemplo, sanciones, procedimientos de respuesta, tecnología) para el acceso físico no autorizado a información, funciones, servicios y activos fundamentales para la misión o el negocio?

Seguridad del personal

6.2 ¿Tiene un proceso para incorporar personal?

6.3 ¿Tiene políticas para realizar verificaciones de antecedentes de sus empleados?

6.6 ¿Tiene un proceso para dar de baja a personal?

6.10 ¿Todo el personal está capacitado en las prácticas recomendadas de seguridad? Esto incluye, entre otros aspectos, amenazas de agentes internos, control de acceso y protección de datos.

6.11 ¿Se proporciona capacitación de seguridad adicional a los usuarios con privilegios elevados (usuarios)?

EJEMPLO DE VULNERABILIDAD Y MÉTODOS PARA ASEGURAR EL ACCESO FÍSICO Y LÓGICO: CASINO HACKEADO A TRAVÉS DEL TERMÓMETRO DE UNA PECERA[vi,vii]

En 2017, un casino agregó un dispositivo “inteligente” aparentemente simple: un termómetro para pecera conectado a Internet. Luego, cibercriminales vulneraron el termómetro, lograron introducirse de manera constante en la red del casino y pudieron extraer información de una base de datos de grandes apostadores. Es tentador atribuir la culpa de esta infracción a errores del fabricante, del proveedor de servicios en la nube y al personal de IT y seguridad del casino; sin embargo, esta es una excelente historia de advertencia para cada parte interviniente en la cadena de suministro.

En el caso del comprador

- Obtenga información sobre los ciclos de actualización y aplicación de parches del software o firmware del fabricante. ¿Se siguen las prácticas recomendadas para

[vi] https://money.cnn.com/2017/07/19/technology/fish-tank-hack-darktrace/index.html

[vii] https://thehackernews.com/2018/04/iot-hacking-thermometer.html

garantizar que las actualizaciones y la aplicación de parches no se puedan vulnerar? Las actualizaciones y la aplicación de parches deben ser oportunos, estar bien documentados y hacer referencia a listas de vulnerabilidades y exposiciones comunes (“CVE”, por sus siglas en inglés), si corresponde.

- El fabricante debe proporcionar suficiente documentación o soporte técnicos para garantizar una implementación segura en su entorno.
- Asegúrese de que sus políticas y procedimientos respalden las prácticas de ciberseguridad e higiene estándar del sector de IT y seguridad para Internet de las cosas (IoT, por su siglas en inglés) o dispositivos de control industrial; por ejemplo, segmentación de red, cambio de credenciales o puertos predeterminados, y monitoreo y alerta de tráfico anómalo.
- El personal interno de IT y Seguridad debe reforzar el acceso físico y lógico a los sistemas críticos y a las cuentas privilegiadas; por ejemplo, acceso físico auditado, principio de privilegio mínimo, y monitoreo y auditoría regular de cuentas o acceso privilegiados.
- Actualice su plan de respuesta a incidentes para incluir los nuevos sistemas. Asegúrese de que el fabricante esté obligado a ofrecer ayuda en la respuesta a incidentes durante un ciberataque que involucre a sus productos.

En el caso del integrador

- Siga las mismas recomendaciones que se indicaron para el comprador.
- Desarrolle estándares para implementar los productos de forma segura en todos los escenarios de uso práctico.
- Diversifique la adquisición, de manera que se incluyan productos de funcionamiento similar con el fin de protegerse contra fallas en la cadena de suministro o vulneraciones de seguridad del producto.
- Proporcione al comprador un documento detallado del alcance del proyecto.
- Proporcione al comprador soporte técnico en asociación con el proveedor.

En el caso del proveedor o fabricante

- Ponga en práctica ciclos de desarrollo de software seguros para el software o firmware del producto. Asegúrese de que se realicen pruebas externas del producto periódicamente y utilice un programa de recompensas por detección de errores.
- Examine los paquetes de hardware para garantizar su seguridad, incluidos los módulos de entrada y salida y los procesadores.
- Ponga en práctica, con los productos, la higiene de ciberseguridad estándar para la conectividad web o basada en la nube. Realice pruebas periódicas utilizando los estándares OWASP.

CASO DE USO 2

APLICACIÓN DE SCRM DE PROVEEDORES A SOLUCIONES ALOJADAS EN LA NUBE

Descripción

Este caso de uso es para aquellos que están considerando el uso de soluciones alojadas en la nube, como la pequeña o mediana empresa (SMB) y la empresa que aloja los servicios en la nube que son clave para las operaciones comerciales (por ejemplo, suites de productividad de colaboración empresarial, herramientas de gestión de relaciones con el cliente, procesamiento de tarjetas de crédito).

Por ejemplo, esto podría ser necesario si un proveedor de servicios subcontrata aspectos de la asistencia al cliente de su servicio de enrutador administrado (como contraseñas de wifi, seguridad, controles parentales, etc.) a un proveedor de la nube. Como otro ejemplo, una SMB podría subcontratar las actividades de marketing a un proveedor de la nube y cargar información PII de los clientes (por ejemplo, nombres, direcciones, números de teléfono) al proveedor de manera regular. En ambos casos, la SMB puede transferir parte del riesgo a los proveedores de la nube, pero debe hacer su debida diligencia al seleccionar dichos proveedores. Seleccionar un proveedor sin aplicar los controles de SCRM adecuados podría poner en riesgo la información de los clientes y, en última instancia, causar daños materiales a la SMB. Es fundamental que las SMB formulen las preguntas correctas al prepararse para entablar estas relaciones.

¿QUÉ RESULTADOS DE DECISIONES RESPALDAN LAS PREGUNTAS?

Este caso de uso es principalmente relevante para los siguientes grupos:

- Comprador: un comprador que considera la seguridad de la cadena de suministro de ICT como parte de su proceso de selección.
- Integrador: una SMB que brinda servicios de integración y que necesita articular y demostrar la debida diligencia adecuada de la postura de SCRM de ICT de las soluciones que está seleccionando o implementando en nombre de sus clientes.

Resultados de la decisiones del comprador

Un comprador utilizará estas preguntas para evaluar los riesgos entre distintos proveedores de soluciones en la nube y asegurarse de que esté plenamente consciente, tenga en cuenta y gestione el entorno de riesgos para cada solución potencial.

Resultados de la decisiones del integrador

Un integrador utilizará estas preguntas para comprender mejor, tener en cuenta y reducir los riesgos al brindar soluciones a uno o más clientes.

Beneficios para el comprador

1. Se garantiza que la SMB conozca las políticas y prácticas de SCRM implementadas por los proveedores de soluciones potenciales.
2. Puede revelar brechas en las prácticas de SCRM del proveedor potencial que la SMB desconocía anteriormente; puede prevenir futuros problemas de SCRM.
3. Se garantiza que las SMB tengan en cuenta los problemas de SCRM que puedan ser relevantes para la obtención de contratos gubernamentales.

4. Proporciona visibilidad sobre los riesgos de la cadena de suministro, que se puede utilizar para la notificación de riesgos, incluso en los contratos.

Beneficios para el integrador

1. Se comunica el compromiso de SCRM del proveedor integrador a los clientes potenciales.
2. Se garantiza la coherencia en la evaluación de posibles soluciones para su uso por parte de las SMB.
3. Se demuestra a las SMB que el integrador está bien informado sobre SCRM.
4. Se proporciona información a las SMB que se puede necesitar rápidamente en caso de un incidente.
5. Proporciona visibilidad sobre los riesgos de la cadena de suministro, que se puede utilizar para la notificación de riesgos, incluso en los contratos.

REFERENCIAS DE LAS PLANTILLAS DE PROVEEDORES (COMPRADOR, INTEGRADOR)

Para ayudar a su organización, las siguientes preguntas se aplican a la mayoría de las SMB y a todos los roles de la cadena de suministro: comprador, integrador o proveedor. Estos no pretenden ser exhaustivos; más bien, son representativos de las prácticas básicas de gestión de riesgos de la cadena de suministro. La Plantilla de Proveedores completa está disponible en https://www.cisa.gov/publication/ict-scrm-task-force-vendor-template.

Plantilla de comprador

Preguntas iniciales

Si puede proporcionar respuestas afirmativas a las siguientes preguntas Y documentación de respaldo vigente, puede omitir TODAS las preguntas restantes.

1.1 ¿Ha proporcionado previamente información sobre gestión de riesgos de la cadena de suministro a esta organización?

Si una SMB utiliza varios casos de uso, puede ser útil identificar preguntas comunes entre ellos. Las respuestas a las preguntas podrían estar entre "sí" y "no".

Si responde "Sí", proporcione una revisión actualizada que cubra los cambios materiales.

O BIEN

1.2 ¿Tiene controles completamente alineados con NIST SP 800-161, Prácticas de gestión de riesgos de la cadena de suministro para los sistemas y organización de información federales?

Si respondió afirmativamente a ALGUNA de las preguntas anteriores, puede adjuntar documentación de respaldo y omitir las preguntas restantes.

Gestión de la cadena de suministro y gobernanza de proveedores

2.3 ¿Tiene una estrategia a nivel de la organización para gestionar los riesgos de toda la cadena de suministro (desde el desarrollo, la adquisición, el soporte del ciclo de vida y la eliminación de sistemas y componentes del sistema hasta los servicios del sistema)?

2.4 ¿Tiene una política o proceso para garantizar que ninguno de sus proveedores ni componentes de terceros estén en alguna lista prohibida?

2.5 ¿Proporciona una lista de materiales (BOM, por sus siglas en inglés) para sus productos, servicios y componentes que incluya todos los elementos lógicos de hardware, firmware y software (por ejemplo, con permisos de lectura, escritura o programación)?

2.6 En el caso de los componentes de hardware incluidos en la oferta de productos, ¿solo los compra a fabricantes de equipos originales o revendedores autorizados?

2.8. ¿Tiene requisitos escritos de Gestión de Riesgos de la Cadena de Suministro (SCRM) en sus contratos con sus proveedores?

Seguridad en el diseño y la ingeniería

3.4. ¿Su organización documenta y comunica los requisitos de control de seguridad para su oferta de hardware, software o soluciones?

3.8. ¿De qué manera su organización previene ataques maliciosos o componentes de propiedad intelectual (IP, por sus siglas en inglés) falsificados dentro de su oferta o solución de productos?

3.11. ¿Su organización verifica que el software de terceros proporcione los requisitos y controles de seguridad requeridos?

3.15. ¿Su organización configura ofertas para implementar configuraciones seguras de forma predeterminada?

3.16. ¿Su organización mantiene y gestiona un programa de respuesta e informes de incidentes de seguridad del producto (PSRT, por sus siglas en inglés)?

Seguridad de la información

4.1. ¿Tiene una autenticación o certificación de seguridad o ciberseguridad válida de terceros (por ejemplo, ISO 27001, SOC 2 tipo 2, CMMC nivel 3-5, evaluación de madurez de ciberseguridad, etc.)? [Si la respuesta es "Sí", indique el programa y la fecha en que recibió la certificación y proporcione una copia de esta. Puede omitir las preguntas restantes de esta sección y pasar a la sección siguiente. Si la respuesta es "No", continúe].

4.2 ¿Sigue estándares o marcos operativos para gestionar la información de seguridad o ciberseguridad (por ejemplo, NIST CSF 1.1, NIST 800-37, Rev. 2, NIST SP 800-161, ISO IEC 27001, ISO 20243, ISO 27036, SAE AS649)?

4.3 ¿Tiene implementadas políticas de seguridad de la información que cubran las políticas de privacidad y estén disponibles públicamente para toda la empresa?

4.4. ¿Realiza un inventario y audita los activos de hardware y software de respaldo o repuesto para garantizar su rendición de cuentas e integridad?

4.6. ¿Tiene procesos o procedimientos establecidos para garantizar que los dispositivos y el software instalados por usuarios externos a su departamento de IT (por ejemplo, personal de la línea de negocios) se detecten, protejan adecuadamente y administren?

4.7. ¿Tiene un programa de gestión de activos que se mantenga regularmente y esté aprobado por la gerencia para sus activos de IT?

4.9. ¿Se asegura de no suministrar a los clientes activos que figuran en una lista prohibida (por ejemplo, ITAR, NDAA sección 889)?

4.11. ¿Tiene políticas o procedimientos documentados para la identificación y detección de amenazas cibernéticas?

4.15. ¿Tiene políticas y procedimientos de control de acceso a la red implementados para sus sistemas de información que estén alineados con los estándares de la industria o los marcos de control?

4.16. ¿Se necesita capacitación en ciberseguridad para el personal que tiene derechos administrativos sobre los recursos informáticos de su empresa?

4.20. ¿Sigue un estándar o marco industrial para sus implementaciones de nube internas o de terceros, si corresponde?

4.21. ¿Tiene prácticas de detección de incidentes definidas y documentadas que describan qué acciones se deben tomar en caso de un evento de seguridad de la información o ciberseguridad?

4.22. ¿Necesita analizar las vulnerabilidades del software que se ejecuta en su empresa antes de su aceptación?

4.23. ¿Implementa software antimalware?

4.24. ¿Tiene un proceso de respuesta a incidentes documentado y un equipo de respuesta a incidentes especializado?

4.26. ¿Tiene procesos o procedimientos para recuperar la funcionalidad completa, incluida la verificación de integridad, después de un incidente importante de ciberseguridad?

Seguridad física

5.2 ¿Tiene políticas y procedimientos de seguridad documentados que aborden el control de acceso físico a activos cibernéticos (dispositivos de red, instalaciones de datos, paneles de conexión, sistemas de control industrial, lógica programable, etc.)?

5.4 ¿Tiene un proceso documentado de respuesta a incidentes de seguridad que cubra incidentes de seguridad física (por ejemplo, posible acceso de intrusos, equipos faltantes, etc.)?

Seguridad del personal

6.1. ¿Existe un programa formal de seguridad del personal?

6.3. ¿Tiene políticas para realizar verificaciones de antecedentes de sus empleados, según lo permita el país en el que opera?

6.4. ¿Tiene políticas para realizar verificaciones de antecedentes de sus proveedores, según lo permita el país en el que opera?

6.5. ¿Tiene políticas para realizar verificaciones de antecedentes de sus subcontratistas, según lo permita el país en el que opera?

6.8. ¿Las prácticas de seguridad del personal se aplican, auditan y actualizan de forma rutinaria?

6.13. ¿Tiene un código de conducta para sus empleados, proveedores y subcontratistas?

Integridad de la cadena de suministro

7.5. ¿Supervisa los productos o servicios de HW y SW de terceros para verificar que no tengan defectos?

7.8. ¿Tiene procesos para evaluar la integridad del producto de posibles proveedores externos durante la selección inicial?

Plantilla de integrador

<u>Preguntas iniciales</u>

Si puede proporcionar respuestas afirmativas a las siguientes preguntas Y documentación de respaldo vigente, puede omitir TODAS las preguntas restantes.

1.1. ¿Ha proporcionado previamente información sobre gestión de riesgos de la cadena de suministro a esta organización?

Si una SMB utiliza varios casos de uso, puede ser útil identificar preguntas comunes entre ellos. Las respuestas a las preguntas podrían estar entre “sí” y “no”.

Si responde “Sí”, proporcione una revisión actualizada que cubra los cambios materiales.

O BIEN

1.2. ¿Tiene controles completamente alineados con NIST SP 800-161, Prácticas de gestión de riesgos de la cadena de suministro para los sistemas y organización de información federales?

Si respondió afirmativamente a ALGUNA de las preguntas anteriores, puede adjuntar documentación de respaldo y omitir las preguntas restantes.

Gestión de la cadena de suministro y gobernanza de proveedores

2.1 ¿Tiene políticas para garantizar la notificación oportuna de la información actualizada de gestión de riesgos que nos proporcionó previamente?

2.3 ¿Tiene una estrategia a nivel de la organización para gestionar los riesgos de toda la cadena de suministro (desde el desarrollo, la adquisición, el soporte del ciclo de vida y la eliminación de sistemas y componentes del sistema hasta los servicios del sistema)?

2.4 ¿Tiene una política o proceso para garantizar que ninguno de sus proveedores ni componentes de terceros estén en alguna lista prohibida?

2.5 ¿Proporciona una lista de materiales (BOM, por sus siglas en inglés) para sus productos, servicios y componentes que incluya todos los elementos lógicos de hardware, firmware y software (por ejemplo, con permisos de lectura, escritura o programación)?

2.6 En el caso de los componentes de hardware incluidos en la oferta de productos, ¿solo los compra a fabricantes de equipos originales o revendedores autorizados?

2.8. ¿Tiene requisitos escritos de Gestión de Riesgos de la Cadena de Suministro (SCRM) en sus contratos con sus proveedores?

Seguridad en el diseño y la ingeniería

3.4. ¿Su organización documenta y comunica los requisitos de control de seguridad para su oferta de hardware, software o soluciones?

3.6. ¿Su organización protege todas las formas de código contra el acceso no autorizado y la manipulación, como las actualizaciones de parches?

3.7. ¿Su organización proporciona un mecanismo para verificar la integridad del lanzamiento de software, incluidas las actualizaciones de parches para su oferta de productos de software?

3.8. ¿De qué manera su organización previene ataques maliciosos o componentes de propiedad intelectual (IP, por sus siglas en inglés) falsificados dentro de su oferta o solución de productos?

3.10. ¿Su organización define, sigue y valida prácticas seguras de codificación y fabricación para mitigar los riesgos de seguridad?

3.11. ¿Su organización verifica que el software de terceros proporcione los requisitos y controles de seguridad requeridos?

3.15. ¿Su organización configura ofertas para implementar configuraciones seguras de forma predeterminada?

3.16. ¿Su organización mantiene y gestiona un programa de respuesta e informes de incidentes de seguridad del producto (PSRT, por sus siglas en inglés)?

Seguridad de la información

4.1. ¿Tiene una autenticación o certificación de seguridad o ciberseguridad válida de terceros (por ejemplo, ISO 27001, SOC 2 tipo 2, CMMC nivel 3-5, evaluación de madurez de ciberseguridad, etc.)?

[Si la respuesta es "Sí", indique el programa y la fecha en que recibió la certificación y proporcione una copia de esta. Puede omitir las preguntas restantes de esta sección y pasar a la sección siguiente. Si la respuesta es "No", continúe].

4.2. ¿Sigue estándares o marcos operativos para gestionar la información de seguridad o ciberseguridad (por ejemplo, NIST CSF 1.1, NIST 800-37, Rev. 2, NIST SP 800-161, ISO IEC 27001, ISO 20243, ISO 27036, SAE AS649)?

4.3. ¿Tiene implementadas políticas de seguridad de la información que cubran las políticas de privacidad y estén disponibles públicamente para toda la empresa?

4.4. ¿Realiza un inventario y audita los activos de hardware y software de respaldo o repuesto para garantizar su rendición de cuentas e integridad?

4.6. ¿Tiene procesos o procedimientos establecidos para garantizar que los dispositivos y el software instalados por usuarios externos a su departamento de IT (por ejemplo, personal de la línea de negocios) se detecten, protejan adecuadamente y administren?

4.7. ¿Tiene un programa de gestión de activos que se mantenga regularmente y esté aprobado por la gerencia para sus activos de IT?

4.8. ¿Tiene políticas o procedimientos documentados para gestionar los activos que se conectan a la red empresarial a lo largo de su ciclo de vida?

4.9. ¿Se asegura de no suministrar a los clientes activos que figuran en una lista prohibida (por ejemplo, ITAR, NDAA sección 889)?

4.10. ¿Tiene políticas y prácticas documentadas de hardware y software para garantizar la integridad de los activos?

4.11. ¿Tiene políticas o procedimientos documentados para la identificación y detección de amenazas cibernéticas?

4.15. ¿Tiene políticas y procedimientos de control de acceso a la red implementados para sus sistemas de información que estén alineados con los estándares de la industria o los marcos de control?

4.16. ¿Se necesita capacitación en ciberseguridad para el personal que tiene derechos administrativos sobre los recursos informáticos de su empresa?

4.17. ¿Incluye obligaciones contractuales para proteger la información y los sistemas de información que manejan sus proveedores?

4.20. ¿Sigue un estándar o marco industrial para sus implementaciones de nube internas o de terceros, si corresponde?

4.21. ¿Tiene prácticas de detección de incidentes definidas y documentadas que describan qué acciones se deben tomar en caso de un evento de seguridad de la información o ciberseguridad?

4.22. ¿Necesita analizar las vulnerabilidades del software que se ejecuta en su empresa antes de su aceptación?

4.23. ¿Gestiona actualizaciones, seguimiento de versiones de nuevos lanzamientos y parches (incluido el historial de parches) para su software y ofertas de servicios de software?

4.24. ¿Implementa software antimalware?

4.25. ¿Tiene un proceso de respuesta a incidentes documentado y un equipo de respuesta a incidentes especializado (Equipo de Respuesta a Incidentes de Seguridad Informática [CSIRT, por sus siglas en inglés])?

4.26. ¿Tiene procesos o procedimientos para recuperar la funcionalidad completa, incluida la verificación de integridad, después de un incidente importante de ciberseguridad?

Seguridad física

5.2. ¿Tiene políticas y procedimientos de seguridad documentados que aborden el control de acceso físico a activos cibernéticos (dispositivos de red, instalaciones de datos, paneles de conexión, sistemas de control industrial, lógica programable, etc.)?

5.3. ¿Tiene políticas documentadas que aborden la capacitación del personal, lo que incluye procedimientos para limitar el acceso físico a activos cibernéticos a solo aquellas personas que tengan una necesidad demostrada?

5.4. ¿Tiene un proceso documentado de respuesta a incidentes de seguridad que cubra incidentes de seguridad física (por ejemplo, posible acceso de intrusos, equipos faltantes, etc.)?

5.5. En el caso de las instalaciones que utilizan un contratista independiente para la seguridad física, ¿las políticas y los procedimientos de seguridad de las instalaciones físicas están incorporados en los acuerdos de nivel de servicio, los contratos, las políticas y las prácticas normativas?

5.10. ¿Tiene procesos establecidos para evitar que ingresen piezas falsificadas a su cadena de suministro?

Seguridad del personal

6.1. ¿Existe un programa formal de seguridad del personal?

6.2 ¿Tiene procesos para incorporar personal?

6.3. ¿Tiene políticas para realizar verificaciones de antecedentes de sus empleados, según lo permita el país en el que opera?

6.4. ¿Tiene políticas para realizar verificaciones de antecedentes de sus proveedores, según lo permita el país en el que opera?

6.5. ¿Tiene políticas para realizar verificaciones de antecedentes de sus subcontratistas, según lo permita el país en el que opera?

6.6. ¿Tiene procesos para dar de baja a personal?

6.8. ¿Las prácticas de seguridad del personal se aplican, auditan y actualizan de forma rutinaria?

6.10. ¿Todo el personal está capacitado en las prácticas recomendadas de seguridad? Esto incluye, entre otros aspectos, amenazas de agentes internos, control de acceso y protección de datos.

6.11. ¿Se proporciona capacitación de seguridad adicional a los usuarios con privilegios elevados?

6.13. ¿Tiene un código de conducta para sus empleados, proveedores y subcontratistas?

Integridad de la cadena de suministro

7.3. ¿Tiene procedimientos documentados de desempeño y validación para sus productos o servicios de HW y SW?

7.4. ¿Tiene procesos implementados para detectar de forma independiente comportamientos anómalos y defectos en sus productos o servicios de HW y SW?

7.5. ¿Supervisa los productos o servicios de HW y SW de terceros para verificar que no tengan defectos?

7.8. ¿Tiene procesos para evaluar la integridad del producto de posibles proveedores externos durante la selección inicial?

Resiliencia de la cadena de suministro

8.3. ¿Cuenta con un plan formal de continuidad empresarial necesario para mantener las operaciones ante interrupciones y pérdidas significativas de personal?

8.5. ¿El personal puede trabajar de forma remota?

EJEMPLO DE VULNERABILIDAD RELACIONADA CON LOS PROVEEDORES DE SERVICIOS EN LA NUBE[viii,ix]

En 2021, un grupo de agentes de amenazas anunció que habían vulnerado los datos de un proveedor de cámaras de seguridad basadas en la nube. Los agentes de amenazas afirmaron haber obtenido acceso a 150,000 cámaras de vigilancia dentro de departamentos de policía, prisiones, escuelas, hospitales y organizaciones privadas. La infracción afectó a empresas conocidas, lo que permitió a los agentes de amenazas acceder a transmisiones en vivo en una serie de áreas confidenciales.

[viii] https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams

[ix] https://www.cyberscoop.com/verkada-breach-surveillance-facial-recognition-privacy/

CASO DE USO 3

EVALUACIÓN DE PROVEEDORES DE SERVICIOS GESTIONADOS (MSP)

Descripción

El objetivo es crear una plantilla para ayudar a las SMB a evaluar a los proveedores de servicios gestionados (es decir, proveedores que tendrán "acceso crítico" [root, superusuario, administrador] a sus sistemas o datos).

El caso de uso de esta plantilla es la selección de un proveedor de servicios gestionados (MSP) para brindar asistencia técnica a una pequeña o mediana empresa (SMB). La SMB tiene un contrato con un cliente grande que es muy particular en cuanto a la gestión de riesgos de la cadena de suministro, y el contrato exige que la SMB gestione los riesgos posteriores a la cadena de suministro introducidos por proveedores que tienen "acceso crítico" a sistemas o datos. Debido a que el MSP instalará y administrará sistemas de hardware y software, es necesario otorgarle al MSP "acceso crítico" (root, superusuario, administrador) a sus sistemas o datos. Por lo tanto, el MSP se enmarca dentro del ámbito del acuerdo contractual con respecto a la gestión de riesgos de la cadena de suministro.

¿QUÉ RESULTADOS DE DECISIONES RESPALDAN LAS PREGUNTAS?

Este caso de uso es principalmente relevante para los siguientes grupos:

- Comprador: un comprador que considera la seguridad de la cadena de suministro de ICT como parte de su proceso de selección.

Resultados de la decisiones del comprador

1. La SMB tiene la tranquilidad de que el MSP comparte su priorización de la seguridad de la cadena de suministro como condición para la adjudicación de un contrato maestro de servicios.
2. La SMB puede demostrar a la gerencia que, al menos con respecto a la gestión general de riesgos empresariales, este aspecto particular del negocio se examinó completamente.
3. La SMB obtiene una mejor perspectiva del perfil de riesgo del MSP para el contrato actual, así como para la comparación con otros MSP en futuras solicitudes de propuestas (RFP, por sus siglas en inglés).

Beneficios para el comprador

1. Se asegura a los directores, inversionistas y aseguradores que se tomaron todas las medidas para garantizar la procedencia de los componentes incluidos en su servicio final.
2. Se proporciona mayor credibilidad al estado de comprador en la industria.
3. Se proporciona un nivel adicional de seguridad y confianza en los servicios del proveedor.
4. Se mejora la calidad actual y futura potencial de la relación entre el proveedor y el comprador.
5. Se mejora la transparencia del proceso.

REFERENCIAS DE LAS PLANTILLAS DE PROVEEDORES (COMPRADOR)

Para ayudar a su organización, las siguientes preguntas se aplican a la mayoría de las SMB y a todos los roles de la cadena de suministro: comprador, integrador o proveedor. Estos no pretenden ser exhaustivos; más bien, son representativos de las prácticas básicas de gestión de riesgos de la cadena de suministro. La Plantilla de Proveedores completa está disponible en https://www.cisa.gov/publication/ict-scrm-task-force-vendor-template.

Plantilla de comprador

Preguntas iniciales

Si puede proporcionar respuestas afirmativas a las siguientes preguntas Y documentación de respaldo vigente, puede omitir TODAS las preguntas restantes.

Si una SMB utiliza varios casos de uso, puede ser útil identificar preguntas comunes entre ellos. Las respuestas a las preguntas podrían estar entre "sí" y "no".

1.1. ¿Ha proporcionado previamente información sobre gestión de riesgos de la cadena de suministro a esta organización?

Si responde "Sí", proporcione una revisión actualizada que cubra los cambios materiales.

O BIEN

1.2. ¿Tiene controles completamente alineados con NIST SP 800-161, Prácticas de gestión de riesgos de la cadena de suministro para los sistemas y organización de información federales?

Si respondió afirmativamente a ALGUNA de las preguntas anteriores, puede adjuntar documentación de respaldo y omitir las preguntas restantes.

Gestión de la cadena de suministro y gobernanza de proveedores

2.1. ¿Tiene políticas para garantizar la notificación oportuna de la información actualizada de gestión de riesgos que nos proporcionó previamente?

2.3. ¿Tiene una estrategia a nivel de la organización para gestionar los riesgos de toda la cadena de suministro (desde el desarrollo, la adquisición, el soporte del ciclo de vida y la eliminación de sistemas y componentes del sistema hasta los servicios del sistema)?

2.4. ¿Tiene una política o proceso para garantizar que ninguno de sus proveedores ni componentes de terceros estén en alguna lista prohibida?

2.7. ¿Tiene un proceso para rastrear y seguir su producto durante el desarrollo y la fabricación?

2.8. ¿Tiene requisitos escritos de Gestión de Riesgos de la Cadena de Suministro (SCRM) en sus contratos con sus proveedores?

2.9. ¿Revisa periódicamente sus requisitos de SCRM escritos para incluir las disposiciones necesarias?

2.10. ¿Tiene políticas para que sus proveedores le notifiquen cuando hay cambios en sus subcontratistas o sus ofertas (componentes, productos, servicios o actividades de soporte)?

Seguridad en el diseño y la ingeniería

3.4. ¿Su organización documenta y comunica los requisitos de control de seguridad para su oferta de hardware, software o soluciones?

3.7. ¿Su organización proporciona un mecanismo para verificar la integridad del lanzamiento de software, incluidas las actualizaciones de parches para su oferta de productos de software?

3.8. ¿De qué manera su organización previene ataques maliciosos o componentes de propiedad intelectual (IP, por sus siglas en inglés) falsificados dentro de su oferta o solución de productos?

3.11 ¿Su organización verifica que el software de terceros proporcione los requisitos y controles de seguridad requeridos?

3.14. ¿Su organización implementa prácticas formales de análisis de vulnerabilidades y debilidades?

3.16. ¿Su organización mantiene y gestiona un programa de respuesta e informes de incidentes de seguridad del producto (PSRT, por sus siglas en inglés)?

Gestión de activos

4.6 ¿Tiene procesos o procedimientos establecidos para garantizar que los dispositivos y el software instalados por usuarios externos a su departamento de IT (por ejemplo, personal de la línea de negocios) se detecten, protejan adecuadamente y administren?

4.9. ¿Se asegura de no suministrar a los clientes activos que figuran en una lista prohibida (por ejemplo, ITAR, NDAA sección 889)?

4.11. ¿Tiene políticas o procedimientos documentados para la identificación y detección de amenazas cibernéticas?

4.15. ¿Tiene políticas y procedimientos de control de acceso a la red implementados para sus sistemas de información que estén alineados con los estándares de la industria o los marcos de control?

4.16. ¿Se necesita capacitación en ciberseguridad para el personal que tiene derechos administrativos sobre los recursos informáticos de su empresa?

4.23. ¿Gestiona actualizaciones, seguimiento de versiones de nuevos lanzamientos y parches (incluido el historial de parches) para su software y ofertas de servicios de software?

4.24. ¿Implementa software antimalware?

4.26. ¿Tiene procesos o procedimientos para recuperar la funcionalidad completa, incluida la verificación de integridad, después de un incidente importante de ciberseguridad?

4.27. ¿Tiene seguro contra daños financieros derivados de un incidente importante de ciberseguridad (por ejemplo, autoseguro, seguro de terceros, empresa matriz, etc.)?

Seguridad física

5.2. ¿Tiene políticas y procedimientos de seguridad documentados que aborden el control de acceso físico a activos cibernéticos (dispositivos de red, instalaciones de datos, paneles de conexión, sistemas de control industrial, lógica programable, etc.)?

5.4. ¿Tiene un proceso documentado de respuesta a incidentes de seguridad que cubra incidentes de seguridad física (por ejemplo, posible acceso de intrusos, equipos faltantes, etc.)?

5.7. ¿Tiene evidencia de que los mecanismos de seguridad física son efectivos y adecuados para proteger los activos? La evidencia podría incluir la evaluación de terceros, la autoevaluación, registros de acciones tomadas para hacer cumplir las normas, etc.

Preguntas sobre la seguridad del personal

6.1. ¿Existe un programa formal de seguridad del personal?

6.6. ¿Tiene procesos para dar de baja a personal?

6.7. ¿Las prácticas de seguridad del personal están documentadas formalmente y son accesibles para todos los empleados?

6.8. ¿Las prácticas de seguridad del personal se aplican, auditan y actualizan de forma rutinaria?

6.9. ¿Se exige al personal que complete una capacitación formal sobre SCRM anualmente?

6.10. ¿Todo el personal está capacitado en las prácticas recomendadas de seguridad? Esto incluye, entre otros aspectos, amenazas de agentes internos, control de acceso y protección de datos.

6.11. ¿Se proporciona capacitación de seguridad adicional a los usuarios con privilegios elevados?

6.12. ¿Conoce las prácticas de capacitación en seguridad que realizan sus subproveedores a su personal?

Integridad de la cadena de suministro

7.1. ¿Sus procesos de integridad del producto se ajustan a alguna de las siguientes normas (por ejemplo, ISO 27036, SAE AS6171, etc.)?

7.2. ¿Controla la integridad de sus prácticas de desarrollo de hardware y software (HW/SW) mediante el uso de prácticas de ciclo de vida de desarrollo seguro?

7.4. ¿Tiene procesos implementados para detectar de forma independiente comportamientos anómalos y defectos en sus productos o servicios de HW y SW?

7.6. ¿La integridad funcional de su producto o servicio depende de servicios en la nube (comerciales o híbridos)?

7.8. ¿Tiene procesos para evaluar la integridad del producto de posibles proveedores externos durante la selección inicial?

7.9. ¿Tiene auditorías programadas periódicamente para garantizar el cumplimiento de los requisitos de integridad de productos o servicios de HW y SW?

Resiliencia de la cadena de suministro

8.1. ¿Su organización tiene un proceso formal para garantizar la resiliencia de la cadena de suministro como parte de sus prácticas de SCRM de la oferta de productos?

8.2. ¿Considera las amenazas no técnicas a la resiliencia de la cadena de suministro, como el clima, la inestabilidad geopolítica, los brotes epidémicos, las erupciones volcánicas, los terremotos, etc.?

8.3. ¿Cuenta con un plan formal de continuidad empresarial necesario para mantener las operaciones ante interrupciones y pérdidas significativas de personal?

8.4. ¿Mantiene un equipo de gestión de crisis especializado y capacitado formalmente, como personal de guardia, asignado para abordar riesgos catastróficos o sistémicos de su cadena de suministro o procesos de fabricación?

8.6. ¿Su empresa considera la diversidad de proveedores para evitar fuentes únicas y reducir la posibilidad de que algunos proveedores sean susceptibles a las mismas amenazas a la resiliencia?

EJEMPLO DE VULNERABILIDAD RELACIONADA CON LOS PROVEEDORES DE SERVICIOS GESTIONADOS [x,xi]

En 2013, un grupo de agentes de amenazas vulneraron al menos 40 millones de cuentas de tarjetas de crédito y débito pertenecientes a consumidores que compraron en varias de las mismas tiendas. Los agentes de amenazas obtuvieron acceso a las redes internas de la tienda a través de un portal de proveedores mediante la vulneración de las credenciales de inicio de sesión de un contratista de refrigeración. Estas credenciales de inicio de sesión robadas permitieron al agente de amenazas obtener acceso confiable a la red de la tienda y extraer datos.

[x] https://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/

[xi] https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

APÉNDICE A: CASO PRÁCTICO PARA EVALUAR A UN PROVEEDOR DE SERVICIOS GESTIONADOS

Desde hace años, varias herramientas operativas de las que dependen las empresas han migrado hacia un modelo de suscripción y se han alejado de la propiedad absoluta por parte de la empresa. El software empresarial común, como Microsoft Word, Excel y PowerPoint, ahora solo está disponible mediante suscripción. Intuit está promocionando considerablemente QuickBooks en línea como una alternativa a sus versiones de escritorio e incentivando el cambio con promociones y funcionalidades mejoradas. Incluso las inversiones en seguridad física de una empresa están pasando de un modelo de inversiones de capital (CapEx) a un modelo de gastos operativos (OpEx) para aprovechar las ofertas de empresas que brindan videovigilancia y control de acceso como un servicio habilitado a través de avances en la tecnología y la adopción de servicios en la nube.

Los beneficios financieros de estos nuevos modelos de servicio para las pequeñas y medianas empresas son reales, especialmente en su capacidad de alinear y correlacionar mejor los gastos y los ingresos de una empresa para mejorar el flujo de caja. También permiten a la empresa realizar mejoras en productividad y eficiencia de forma inmediata sin tener que financiar grandes inyecciones de capital que solían ser necesarias. Sin embargo, estos servicios pueden crear vulnerabilidades cibernéticas que las SMB deben revisar y mitigar. Este marco se puede utilizar para evaluar ofertas de servicios con la misma eficacia con la que se evalúan las inversiones de capital tradicionales.

En este ejemplo, una SMB busca instalar un sistema de seguridad física en sus instalaciones de oficina. Las medidas de seguridad física son importantes para proteger al personal y la propiedad de intrusiones no deseadas. En un entorno competitivo, las medidas de seguridad física también pueden ayudar a proteger y salvaguardar la propiedad intelectual de una empresa, y posicionar a una SMB como un proveedor confiable para sus clientes posteriores, especialmente si esos clientes son contratistas directos o indirectos de entidades gubernamentales.

Las ofertas de seguridad física disponibles en la actualidad incluyen equipos locales vendidos a través de distribuidores y revendedores de valor agregado (VAR, por sus siglas en inglés), así como modelos de suscripción en los que se entregan equipos y software de gestión a cambio de una tarifa de suscripción mensual o anual. En este ejemplo, el Grupo de Trabajo analizará específicamente el modelo de suscripción de un sistema de videovigilancia.

Los sistemas de videovigilancia constan de cámaras montadas en toda una instalación (exterior e interior), almacenamiento de las secuencias de video y software utilizado para la búsqueda y recuperación de dichas secuencias. En la mayoría de los modelos de suscripción, las cámaras transmiten las imágenes a un almacenamiento alojado en la nube de un cliente de software capaz de administrar el estado de las cámaras, buscar y recuperar imágenes almacenadas y procesar alarmas. Las SMB que utilizan estos servicios evitan el costo inicial del equipo y la mano de obra de instalación, así como los costos continuos de mantenimiento de servidores de almacenamiento y las molestias de los parches de software. Sin embargo, al hacerlo, aceptan la noción de que las imágenes de sus instalaciones y su personal se almacenarán en algún lugar de una nube pública, y confían en las medidas de seguridad del proveedor para garantizar la confidencialidad adecuada. En la siguiente sección, se presentan ejemplos de cómo se puede utilizar el marco para evaluar a posibles proveedores.

REFERENCIAS DE LAS PLANTILLAS DE PROVEEDORES (COMPRADOR)

2.3. *¿Tiene una estrategia a nivel de la organización para gestionar los riesgos de toda la cadena de suministro (desde el desarrollo, la adquisición, el soporte del ciclo de vida y la eliminación de sistemas y componentes del sistema hasta los servicios del sistema)?*

(Los servicios de videovigilancia generalmente dependen de infraestructuras de nube pública. Es importante comprender dónde se almacena físicamente la información de sus instalaciones, durante cuánto tiempo y quién tiene acceso a los datos, ya que las vulnerabilidades y los ataques a estas plataformas pueden afectar el perfil de riesgo cibernético de su empresa).

[Sí, No, Otro o N/C]

Respuestas apropiadas: “Sí” u “Otro”. Lo ideal sería que un proveedor adecuado contara con procesos y procedimientos establecidos para garantizar la procedencia de los componentes del sistema y para controlar la cadena de custodia de los componentes a lo largo de su ciclo de vida, incluido el retiro y la eliminación adecuados de dichos componentes.

2.3.1. *¿Cuál es su estrategia?*

Respuestas apropiadas: un proveedor adecuado debería tener, como mínimo, una estrategia implementada que se ajuste a las prácticas recomendadas de la industria y a las pautas establecidas para gestionar los riesgos de la cadena de suministro, como las descritas por la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) y el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés). Un proveedor debe afirmar que cumple con los principios descritos en el marco de riesgo de servicios gestionados de IT de CISA.

2.3.2. *¿De qué manera lo implementó?*

Respuestas apropiadas: un proveedor adecuado debería poder demostrar cómo se implementa el proceso dentro de la organización, incluida la capacitación regular y la educación del personal.

2.4. *¿Tiene una política o proceso para garantizar que ninguno de sus proveedores ni componentes de terceros estén en alguna lista prohibida?*

Sanciones gubernamentales (por ejemplo, la Ley de Autorización de Defensa Nacional de los Estados Unidos [NDAA, por sus siglas en inglés] de 2018) estipula ciertas entidades comerciales que no pueden ser utilizadas en redes gubernamentales ni por contratistas gubernamentales. Dado que los equipos suministrados en los servicios de vigilancia pueden venir incluidos en el servicio y no comprarse por separado, es importante asegurarse de que no provengan de entidades sancionadas.

Respuestas apropiadas: “Sí”. Una organización adecuada tendría, como mínimo, conocimiento de los servicios y equipos de telecomunicaciones prohibidos de conformidad con la NDAA de 2019 (Ley de Autorización de Defensa Nacional John S. McCain para el Año Fiscal 2019) y las acciones relacionadas con ello por parte del Departamento de Comercio (Department of Commerce) y la Comisión Federal de Comunicaciones. De igual forma, el proveedor debe tener conocimiento de las acciones del Departamento de Energía (Department of Energy) con respecto al control de supervisión y adquisición de datos (SCADA, por sus siglas en inglés) y los sistemas de control industrial para hardware controlado o prohibido.

2.7. *¿Tiene un proceso para rastrear y seguir su producto durante el desarrollo y la fabricación?*

[Sí, No, Otro o N/C]

Respuestas apropiadas: “Sí” u “Otro”. Un proveedor adecuado tendría conocimiento de la situación de la producción y el abastecimiento de piezas de los fabricantes posteriores, incluido un conocimiento profundo del proceso de desarrollo.

2.7.1. *¿Cómo realizar el seguimiento de su cadena de custodia?*

Respuestas apropiadas: una respuesta apropiada demostraría haber establecido una estrecha relación de trabajo con los fabricantes de componentes, lo que, a su vez, estaría acompañado de visibilidad de los procesos de esos proveedores para garantizar la procedencia de los componentes, así como la integridad de esos componentes desde el ensamblaje, el embalaje y la distribución o la entrega.

2.7.2. *¿Cómo se realiza el seguimiento y rastreo de los componentes dentro de su producto?*

Respuestas apropiadas: un proveedor adecuado debe tener la capacidad de rastrear y seguir cada componente que forma parte del producto, desde los proveedores y fabricantes hasta el ensamblaje y la entrega final a los clientes. La trazabilidad es "la capacidad de rastrear los antecedentes, la aplicación o la ubicación de una entidad mediante identificaciones registradas".[xii] En concreto, el proveedor debería utilizar códigos de barras e identificación por radiofrecuencia (RFID, por sus siglas en inglés) como práctica estándar. Lo ideal sería que el proceso utilizado fuera automático, con la capacidad de correlacionar varios datos sobre el componente a medida que se mueve a través de las cadenas de suministro y entrega.

3.7. *¿Su organización proporciona un mecanismo para verificar la integridad del lanzamiento de software, incluidas las actualizaciones de parches para su oferta de productos de software?*

(Uno de los beneficios de utilizar software basado en la nube en lugar de comprarlo es que los propios proveedores pueden realizar actualizaciones de forma automática y global. Es importante comprender aspectos como la frecuencia de lanzamiento de parches del proveedor y los acuerdos de nivel de servicio [SLA] con respecto al tiempo que transcurre desde la identificación de la vulnerabilidad hasta el lanzamiento del parche, etc.).

Respuestas apropiadas: "Sí" u "Otro". Un proveedor adecuado debería poder señalar los estándares de codificación de la organización, es decir, el conjunto de reglas de codificación, pautas y prácticas recomendadas que la ayuden a garantizar que el software en cuestión sea seguro y confiable. El proveedor también debería poder señalar las iniciativas internas que ha tomado para capacitar al personal clave apropiado sobre cuáles son esos estándares de codificación y cómo implementarlos de la mejor manera.

3.8. *¿De qué manera su organización previene ataques maliciosos o componentes de propiedad intelectual (IP, por sus siglas en inglés) falsificados dentro de su oferta o solución de productos?*

Respuestas apropiadas: "Sí" u "Otro". De manera similar a lo anterior, un proveedor adecuado debe tener un proceso implementado que utilice alguna forma de trazabilidad de componentes para proteger sus líneas de producción (incluidos los proveedores posteriores) de la amenaza de componentes o piezas falsificadas. Se trata de un problema de integridad de la cadena de suministro y de ciberseguridad, además de un problema básico de control de calidad. El proveedor debe tener conocimiento de los proveedores de componentes no fiables. La organización debe contar con capacitación para educar al personal sobre cómo identificar y probar componentes de propiedad intelectual maliciosos o falsificados. Lo ideal sería que la organización tuviera una política de tolerancia cero frente a las falsificaciones, y se asegure de utilizar únicamente canales de suministro autorizados.

3.11. *¿Su organización verifica que el software de terceros proporcione los requisitos y controles de seguridad requeridos?*

Respuestas apropiadas: "Sí".

3.14. *¿Su organización implementa prácticas formales de análisis de vulnerabilidades y debilidades?*

Respuestas apropiadas: "Sí" u "Otro".

3.16. *¿Su organización mantiene y gestiona un programa de respuesta e informes de incidentes de seguridad del producto (PSRT, por sus siglas en inglés)?*

Respuestas apropiadas: "Sí" u "Otro".

[xii] EN ISO 8402 (1994) Gestión de la calidad y garantía de la calidad: Vocabulario

4.11 *¿Tiene políticas o procedimientos documentados para la identificación y detección de amenazas cibernéticas?*

(Desafortunadamente, la mayoría de las vulneraciones de datos pasan desapercibidas para la red víctima hasta que un cliente o una entidad externa notifica a los propietarios. No es raro que una infracción pase desapercibida durante seis meses o más antes de que se reciba una notificación y se investigue la evidencia de la infracción. Mantener canales de comunicación abiertos con los proveedores de su cadena de suministro puede ayudar a agilizar las notificaciones y permitirle tomar las medidas adecuadas para subsanar la vulnerabilidad y mitigar el daño potencial).

Respuestas apropiadas: "Sí" u "Otro"

4.11.1. *¿Qué procesos tiene implementados para detectar rápidamente las amenazas cibernéticas?*

Las respuestas apropiadas pueden incluir que equipos de evaluación de seguridad interna auditen periódicamente el software de una empresa. Una empresa también podría suscribirse a un foro de información público (como CISA) para recibir actualizaciones sobre amenazas y notificaciones de procesos. Para ello, deberían verificar sus bibliotecas de compilación de software y realizar un análisis para garantizar que los parches se apliquen correctamente.

4.11.1.1 *¿Cómo gestiona la identificación de amenazas dentro de su cadena de suministro, incluidos proveedores y subcontratistas?*

Una respuesta apropiada puede incluir acuerdos contractuales con los proveedores de software, mediante los cuales se les exija a los proveedores que notifiquen a las pequeñas y medianas empresas si se produce una infracción, o bien un SLA que establezca claramente cuánto tiempo debe pasar antes de que un proveedor esté obligado a publicar un parche de seguridad después de que se haga pública una vulnerabilidad.

4.11.1.2. *¿Qué procesos existen para actuar ante la recepción de información externa creíble sobre amenazas cibernéticas?*

Las respuestas apropiadas pueden incluir la revisión de todas las alertas de dominio público sobre vulnerabilidades conocidas y la publicación de una declaración sobre si la vulnerabilidad afecta el producto de un proveedor.

4.15 *¿Tiene políticas y procedimientos de control de acceso a la red implementados para sus sistemas de información que estén alineados con los estándares de la industria o los marcos de control?*

Respuestas apropiadas: "Sí" u "Otro"

4.15.1. *Si la respuesta es "Sí", enumere las normas o marcos utilizados.*

Las respuestas apropiadas pueden incluir seguir las pautas y los marcos del NIST o utilizar una herramienta de análisis de vulnerabilidad de red actualizada para realizar análisis de forma rutinaria en busca de vulnerabilidades conocidas.

4.15.2. *¿Cuáles son sus prácticas con respecto a elementos como la federación, los usuarios privilegiados y el control de acceso basado en roles para los dispositivos de los usuarios finales?*

Las respuestas apropiadas pueden incluir el uso de listas de control de acceso (ACL, por sus siglas en inglés) para administrar quién tiene acceso a sistemas vitales o la implementación de herramientas de monitoreo de red para detectar si se eleva un privilegio y en qué momento.

4.15.2.1. *¿Cómo se garantiza que se gestione el acceso remoto para los dispositivos de los usuarios finales o los empleados y proveedores, incluida la desactivación de cuentas (por ejemplo, autorización multifactor, cifrado, protección contra malware, etc.)?*

Las respuestas apropiadas pueden incluir el uso de VPN para proteger todo acceso remoto a la red del proveedor, así como el registro de todo acceso de terceros que no sean empleados a los activos de red de la empresa y la desactivación de esas conexiones una vez que se haya completado la tarea.

4.15.2.2. *¿Cómo identifica y corrige los sistemas de usuarios finales que no cumplen con las normas?*

Las respuestas apropiadas pueden incluir la ejecución de análisis de red para identificar direcciones de control de acceso a medios (MAC, por sus siglas en inglés) desconocidas; la implementación de políticas en torno a la seguridad "Traiga su propio dispositivo" (BYOD, por sus siglas en inglés) o la presencia de redes segmentadas para proteger el acceso a servidores y dispositivos informáticos críticos y sus permisos.

4.16. *¿Se necesita capacitación en ciberseguridad para el personal que tiene derechos administrativos sobre los recursos informáticos de su empresa?*

La respuesta apropiada es "Sí". Tenga cuidado con los proveedores que respondan negativamente.

4.16.1. *¿Cuál es la frecuencia de verificación del cumplimiento de la capacitación del personal?*

Las respuestas apropiadas incluirían un cronograma de la frecuencia con la que el personal debe completar esta capacitación, la frecuencia con la que se actualiza la capacitación y la manera en que la organización exige el cumplimiento.

4.16.2. *¿Qué capacitación en ciberseguridad se exige a las partes interesadas externas (por ejemplo, proveedores, clientes, socios, etc.) que tienen acceso a la red?*

Las respuestas apropiadas pueden incluir la separación de terceros e invitados para que solo puedan acceder a una red de invitados o permitirles el acceso solo a los sistemas necesarios de la red principal con privilegios básicos.

4.16.2.1. *¿Cómo se realiza el seguimiento del cumplimiento de la capacitación de terceros con acceso a la red?*

(Durante una reciente y muy publicitada vulneración de un proveedor de servicios en la nube y video, se determinó que varios empleados de la empresa afectada tenían derechos de acceso de superadministrador a los sistemas vendidos e instalados en los sitios de los clientes sin que los clientes lo supieran).[xiii]

La respuesta apropiada incluye la confirmación de múltiples herramientas para realizar el seguimiento del cumplimiento de los empleados y la finalización de la capacitación cibernética.

[xiii] https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams

4.23. *¿Gestiona actualizaciones, seguimiento de versiones de nuevos lanzamientos y parches (incluido el historial de parches) para su software y ofertas de servicios de software?*

Respuesta apropiada: "Sí" u "Otro" (la opción "Otro" solo es aceptable si el proveedor utiliza un tercero o un MSP externo para administrar su red y parches de software).

> 4.23.1 *¿Cuál es la responsabilidad del usuario final del producto (cliente) en cuanto a la actualización de las versiones de software?*
>
> Las respuestas apropiadas pueden incluir la implementación de parches y actualizaciones mediante una herramienta de administración de red central. Busque indicios de una capacidad de administración para detectar la versión del software que se ejecuta en diferentes dispositivos y aplicar reglas de red contra aquellos a los que no se les hayan aplicado parches. Se produce una cantidad significativa de infracciones cuando un sistema o servidor no se ha actualizado con el último parche de seguridad, lo que deja una vulnerabilidad que un atacante puede aprovechar.

4.26 *¿Tiene procesos o procedimientos para recuperar la funcionalidad completa, incluida la verificación de integridad, después de un incidente importante de ciberseguridad?*

Respuestas apropiadas: "Sí" u "Otro". El proveedor debe incluir detalles de los sistemas y planes de continuidad del negocio, incluidas copias de seguridad automáticas de bases de datos y servidores críticos.

> 4.26.1. *¿Cuál es la frecuencia de prueba de los medios de respaldo?*

Las respuestas apropiadas pueden incluir frecuencias semanales o mensuales.

4.27 *¿Tiene seguro contra daños financieros derivados de un incidente importante de ciberseguridad (por ejemplo, autoseguro, seguro de terceros, empresa matriz, etc.)?*

(Si bien existe un seguro contra ataques cibernéticos, su adopción aún no está tan extendida. Las regulaciones en ciertas jurisdicciones (y especialmente en Europa) están diseñadas para proteger a los clientes de una empresa en caso de que esta sea víctima de un ciberataque. Estas regulaciones responsabilizan a la empresa por los daños ocasionados por el robo de información de identificación personal de los clientes de esa empresa. Busque proveedores que comprendan los riesgos que puede enfrentar su empresa y que estén expuestos a las mismas regulaciones o tengan seguro para cubrir sus daños en caso de que la infracción se produzca a través de su oferta de productos).

Respuestas apropiadas: "Sí" u "Otro".

> 4.27.1 *¿La cobertura incluye el daño financiero a sus clientes como resultado de una infracción de ciberseguridad que haya afectado a su empresa?*
>
> Respuestas apropiadas: Idealmente, "Sí" u "Otro". Sin embargo, la respuesta a esta pregunta puede depender de si un instrumento de seguro en particular incluye disposiciones para la cobertura del cliente que no se requieren como estándar de prácticas recomendadas ampliamente aceptado para la ciberseguridad.

6.1. *¿Existe un programa formal de seguridad del personal?*

Respuesta apropiada: "Sí". Una empresa que proporciona equipos y servicios de videovigilancia debe poder proporcionar (y estar dispuesta a hacerlo) detalles de su programa formal de seguridad del personal a la SMB. Una SMB que adquiera dichos equipos y servicios no debería poner en riesgo sus propias operaciones a través de una empresa que no cuente con un programa formal de seguridad del personal.

6.1.1. *¿El acceso de los empleados se gestiona por rol?*

Respuesta apropiada: "Sí". Administrar el acceso por roles es una buena práctica estándar que permite el acceso con el mínimo privilegio. Una respuesta negativa puede indicar que la empresa que proporciona equipos y servicios a la SMB no puede identificar, gestionar ni limitar adecuadamente el acceso a las personas de forma apropiada.

6.1.2. *¿Se gestiona y mantiene formalmente el acceso a sistemas, instalaciones de fabricación y activos críticos para el negocio? Describa el proceso.*

Respuesta apropiada: "Sí". Es esencial que una empresa que proporciona equipos y servicios de videovigilancia a una SMB gestione y mantenga formalmente el acceso a los sistemas, las instalaciones y los activos críticos para el negocio. Si un proveedor de equipos y servicios de videovigilancia no administra ni mantiene formalmente el acceso a sus sistemas, instalaciones y activos críticos para el negocio, una SMB que contrata o se suscribe a los equipos y servicios de esa empresa se expone a sí misma y expone a sus propias operaciones a un riesgo considerable frente a piratas informáticos o a las propias amenazas internas de esa empresa.

6.6. *¿Tiene procesos para dar de baja a personal?*

Respuesta apropiada: "Sí". Nuestro proceso de incorporación y baja del personal se gestiona de forma conjunta entre nuestros Departamentos de IT y RR. HH. Nuestro Departamento de IT utiliza un sistema de gestión de activos de IT que asigna activos y cuentas a los empleados. Una empresa que proporciona equipos y servicios de videovigilancia debe poder proporcionar (y estar dispuesta a hacerlo) detalles del proceso de baja de personal a la SMB. Una SMB que adquiera dichos equipos y servicios no debería poner en riesgo sus propias operaciones a través de una empresa que no cuente con proceso de baja de personal.

6.6.2. *¿Cuál es el proceso para eliminar el acceso a todos los documentos, aplicaciones, activos, etc. de la empresa?*

Respuesta apropiada: Nuestro proceso de baja de personal requiere la interrupción de todo acceso a los documentos, los sistemas, las aplicaciones y las cuentas de la empresa a más tardar a las 5:00 p.m. (hora local) del último día de trabajo del empleado. El empleado y su supervisor son responsables de notificar a nuestro Departamento de IT a más tardar 72 horas antes del último día de trabajo del empleado, o de inmediato, cuando no sea posible notificar con 72 horas de anticipación.

6.6.3. *¿Cuál es el proceso para recuperar todos los activos de la empresa?*

Respuesta Apropiada: Los empleados son responsables de los activos de la empresa que se les entregan y el Departamento de IT mantiene recibos de tenencia mediante el sistema de gestión de activos. Cuando se notifica el despido de un empleado, el Departamento de IT programa una cita con el empleado para que devuelva los activos de la empresa. Si el empleado no devuelve los activos en el momento programado, nuestro Departamento de IT revocará inmediatamente todo acceso del empleado a los sistemas, redes y cuentas. Luego, informamos al empleado y al supervisor. Si un empleado interno no devuelve los activos de la empresa antes del final de su último día, o por correo dentro de un plazo de 7 días en el caso de los empleados que trabajan de manera remota, la empresa toma medidas más firmes de manera progresiva (que pueden incluir acciones legales).

6.10. *¿Todo el personal está capacitado en las prácticas recomendadas de seguridad? Esto incluye, entre otros aspectos, amenazas de agentes internos, control de acceso y protección de datos.*

Respuesta apropiada: "Sí". Contamos con un amplio protocolo de capacitación para todos los empleados. La capacitación en seguridad es obligatoria para todos los empleados nuevos y se exige como capacitación de actualización para todos los empleados de manera anual.

6.11. *¿Se proporciona capacitación de seguridad adicional a los usuarios con privilegios elevados?*

Respuesta apropiada: "Sí". Absolutamente. Se requiere capacitación en seguridad adicional como parte esencial de nuestro Programa de Gestión de Acceso Privilegiado. Esta capacitación es necesaria para que las personas obtengan y mantengan acceso a cuentas privilegiadas.

7.6. *¿La integridad funcional de su producto o servicio depende de servicios en la nube (comerciales o híbridos)?*

Respuesta apropiada: "Sí" o "No" son respuestas aceptables. El punto clave es que la empresa conozca los componentes y la procedencia de su producto o servicio.

> 7.6.1. *¿Qué políticas y procedimientos existen para proteger la integridad de los datos proporcionados a través de los servicios en la nube?*
>
> Respuesta apropiada: Al seleccionar un proveedor de servicios en la nube, investigamos si las empresas segmentaban las redes de máquinas virtuales para diferentes clientes. Internamente, protegemos los datos de nuestros clientes mediante la aplicación de software de seguridad (incluido antivirus), mantenimiento de parches, minimización de privilegios y encriptación de comunicaciones.

APÉNDICE B: REFERENCIAS

CYBER ESSENTIALS[1]

- Conceptos básicos sobre ciberseguridad (Cyber Essentials) de CISA es una guía para líderes de pequeñas empresas, así como para líderes de agencias gubernamentales pequeñas y locales, para desarrollar una comprensión práctica de dónde comenzar a implementar prácticas de ciberseguridad organizacional.

CYBER ESSENTIALS STARTER KIT[2]

- El Kit de inicio de conceptos básicos sobre ciberseguridad (Cyber Essentials Starter Kit) es un conjunto de módulos que los líderes y su personal pueden usar como punto de partida para construir una cultura de preparación cibernética consistente con el marco de ciberseguridad del NIST y otros estándares.

CYBERSECURITY RESOURCES ROAD MAP[3]

- La Hoja de ruta de recursos sobre ciberseguridad (Cybersecurity Resources Road Map) está diseñada para ayudar a las pequeñas y medianas empresas con infraestructura crítica a identificar recursos de ciberseguridad útiles para satisfacer sus necesidades.

HEALTH INDUSTRY CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT GUIDE (HIC- SCRIM)[4]

- El Grupo de Trabajo Conjunto sobre Ciberseguridad (JCWG, por su siglas en inglés) del Consejo de Coordinación del Sector de Salud y Salud Pública (HSCC, por sus siglas en inglés) desarrolló esta guía de gestión de riesgos de ciberseguridad de la cadena de suministro para brindar estructura y ayuda como una herramienta dirigida a organizaciones de salud pequeñas y medianas.

NASA SEWP V TRAINING VIDEO - OPEN TRUSTED TECHNOLOGY PROVIDER STANDARD CERTIFICATION - ISO 20243[5]

- La Administración Nacional de Aeronáutica y el Espacio (NASA, por sus siglas en inglés) creó un video de capacitación sobre la norma ISO 20243, también conocida como Certificación Estándar de Proveedor de Tecnología de Confianza Abierta (O-TTPS, por sus siglas en inglés), creada por The Open Group.

NIST CYBERSECURITY PRACTICE GUIDE SP 1800-15[6]

- La guía SP 1800-15 brinda una descripción para los desarrolladores e implementadores de productos de IoT de cuatro implementaciones diferentes que utilizan la Descripción de uso del fabricante (MUD, por sus siglas en inglés) a fin de limitar automáticamente los dispositivos de IoT para que envíen y reciban solo el tráfico que necesitan para realizar las funciones previstas.

SECURITY POLICY TEMPLATES[7]

- SANS ha desarrollado y publicado aquí un conjunto de plantillas de políticas de seguridad.

SOLUTIONS FOR ENTERPRISE WIDE PROCUREMENT (SEWP) ISO 20243 (SCRM)[8]

- La norma ISO 20243, también conocida como Certificación Estándar de Proveedor de Tecnología de Confianza Abierta (O-TTPS) fue creada por The Open Group.

STOP.THINK.CONNECT[9]

- Stop.Think.Connect es una campaña global de concientización sobre seguridad en Internet que incluye recursos y materiales para ayudar a mantener la ciberseguridad de su pequeña empresa.

APÉNDICE C: PREGUNTAS EN FORMATO ALTERNATIVO

HOJA DE CÁLCULO DE EXCEL[10]

- El Grupo de Trabajo desarrolló una hoja de cálculo como herramienta alternativa, destinada a permitir opciones de respuestas afirmativas, negativas o parciales a cada una de las preguntas seleccionadas en la guía.

CONTACTO DEL DHS

Centro Nacional de Gestión de Riesgos (NRMC, por sus siglas en inglés)

Agencia de Seguridad Cibernética y de Infraestructura (Cybersecurity and Infrastructure Security Agency)
U.S. Department of Homeland Security
NRMC@hq.dhs.gov
Para obtener más información sobre NRMC, visite www.cisa.gov/national-risk-management

---

1 https://www.cisa.gov/cyber-essentials
2 https://www.cisa.gov/sites/default/files/publications/Cyber Essentials Starter Kit_03.12.2021_508_0.pdf
3 https://us-cert.cisa.gov/resources/smb
4 https://healthsectorcouncil.org/hic-scrim-v2/
5 https://www.youtube.com/watch?v=dmLEDkXqEkQ
6 https://csrc.nist.gov/News/2021/mitigating-network-based-attacks-on-iot-devices-us
7 https://www.sans.org/information-security-policy/
8 https://www.sewp.nasa.gov/iso_20243.shtml
9 https://www.cisa.gov/publication/stopthinkconnect-small-business-resources
10 https://www.cisa.gov/ict-scrm-task-force