CAPACITAR A LAS SMB:
GUÍA DE RECURSOS PARA EL DESARROLLO DE UN PLAN DE GESTIÓN DE RIESGOS RESILIENTE PARA LA CADENA DE SUMINISTRO

INTRODUCCIÓN

En esta guía de recursos, se aborda la creciente necesidad de que las pequeñas y medianas empresas (SMB) de tecnologías de la información y las comunicaciones (ICT) presenten un plan de gestión de riesgos de la cadena de suministro (SCRM) para las partes interesadas del sector público o privado. El objetivo es garantizar la disponibilidad, integridad y confidencialidad de los productos, servicios y componentes de las ICT a lo largo de la cadena de suministro, de modo que se reduzcan al mínimo las interrupciones y las vulnerabilidades.

La Administración de Pequeñas Empresas de los Estados Unidos (U.S. Small Business Administration) define una pequeña y mediana empresa según un conjunto de estándares basados en industrias específicas. Generalmente, estos estándares de tamaño se basan en la cantidad de empleados o en la cantidad de ingresos anuales de la empresa.[1] A los efectos de este documento, se define como SMB de ICT a una organización con menos de 500 empleados.[2] Dado que reconocemos que muchas SMB de ICT carecen de experiencia específica sobre la gestión de riesgos o SCRM, esta guía ofrece un valioso punto de partida para que las SMB de ICT desarrollen y adapten su propio plan de SCRM de ICT.

Aunque se centra principalmente en los sectores de tecnología de la información y las comunicaciones, esta guía es de interés para las SMB de cualquier industria. Al utilizar este recurso y participar activamente en la SCRM, las SMB pueden desarrollar un plan de SCRM viable para mitigar el riesgo de interrupción en su cadena de suministro, mejorar la resiliencia de su cadena de suministro y satisfacer posibles solicitudes de los procesos de adquisición de las partes interesadas.

1 U.S. Small Business Administration. “Size standards.” Última actualización: 21 de junio de 2023. https://www.sba.gov/federal-contracting/contracting-guide/size-standards. Consultado el 7 de agosto de 2023.
2 U.S. Chamber of Commerce. (10 de abril de 2023) “The State of Small Business Now.” https://www.uschamber.com/small-business/state-of-small-business-now

FUNCIONES CLAVE

Las SMB del sector de las ICT suelen desempeñar distintas funciones en el transcurso de sus actividades comerciales. En consecuencia, su organización debe tener en cuenta las siguientes funciones al desarrollar un plan de SCRM de ICT.

COMPRADOR

Propietario, operador o directivo de una SMB que desea realizar una compra en la que la seguridad de la cadena de suministro de las 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 las ICT es motivo de preocupación para el potencial cliente.

ELEMENTOS DEL PLAN

01 EMPEZAR CON UN RESUMEN EJECUTIVO

ORIENTACIÓN Y PASOS A SEGUIR

Su plan de SCRM de las ICT debe comenzar con un breve resumen ejecutivo. Debe incluir una descripción general del propósito, las metas, los objetivos y los elementos clave de su plan.

02 IDENTIFICAR LOS PROVEEDORES CRÍTICOS

ORIENTACIÓN Y PASOS A SEGUIR

Identifique a los proveedores que proporcionan hardware o software a su empresa, o tienen acceso a estos, como servicios en la nube, mediante las siguientes acciones:

I. Crear y mantener una lista de proveedores, especialmente aquellos que son críticos para sus operaciones comerciales, y evaluar su importancia en términos de resultados en su negocio.

II. Identificar y priorizar los posibles riesgos que plantean los proveedores críticos.

III. Establecer un proceso formal para actualizar las evaluaciones de riesgos de sus proveedores críticos, y para identificar y recibir notificación de posibles vulnerabilidades, como inestabilidad financiera, riesgos de ciberseguridad o riesgos para la reputación.

03 IDENTIFICAR LOS RIESGOS DE LA CADENA DE SUMINISTRO PARA SUS ACTIVOS CRÍTICOS

ORIENTACIÓN Y PASOS A SEGUIR

Los equipos y servicios de ICT están compuestos por muchos componentes (críticos y no críticos), cuyo suministro a menudo está a cargo de un gran número de proveedores, comúnmente conocidos como la “cadena de suministro”. Para saber qué activos o proveedores críticos (si se interrumpen o se ven comprometidos) afectarán negativamente sus operaciones comerciales, debe hacer lo siguiente:

I. Identificar y priorizar el hardware y el software que se utilizan en sus operaciones.

II. Establecer un método para recibir notificaciones sobre parches y actualizaciones disponibles para su hardware y software, y aplicarlos rápidamente.

III. Identificar la fecha de finalización de la vida útil del hardware y el software, y planificar una transición oportuna a hardware y software actualizados siempre que sea posible.

ELEMENTOS DEL PLAN

04 CONTAR CON UNA DIVERSIDAD DE PROVEEDORES

ORIENTACIÓN Y PASOS A SEGUIR

Mantener, siempre que sea posible, una base de proveedores diversa reducirá su dependencia de un solo proveedor. Por el contrario, depender de un único proveedor crítico puede aumentar el riesgo para su organización si los productos o servicios críticos dejan de estar disponibles. Esto puede incluir el uso de servicios de ciberseguridad proporcionados por un tercero. Para lograrlo, debe hacer lo siguiente:

I. Desarrollar criterios de calificación de proveedores que garanticen que todos sus proveedores suministren constantemente productos y servicios de calidad.
II. Fomentar relaciones sólidas con sus proveedores y mantener una comunicación abierta para abordar cualquier problema o inquietud que pueda surgir.
III. Identificar puntos únicos de falla en su cadena de suministro y proveedores alternativos en caso de que un proveedor no cumpla con sus requisitos contractuales.

05 DESARROLLAR UN PROCESO DE CERTIFICACIÓN DE PROVEEDORES

ORIENTACIÓN Y PASOS A SEGUIR

Las decisiones que repercuten en la cadena de suministro podrían afectar todas las áreas de su negocio. Estas incluyen la decisión de comprar o utilizar productos, sistemas o servicios. Para evaluar a los proveedores antes de realizar una compra y mantener su calidad conforme avanza el tiempo, su organización debe implementar procesos y documentación mediante los cuales los proveedores certifiquen, desde el principio y periódicamente a partir de entonces, atributos específicos de la gestión de riesgos. Las formas de lograrlo son las siguientes:

I. Establecer acuerdos de nivel de servicio.
II. Realizar auditorías periódicas a los proveedores para garantizar que cumplan con sus políticas y procedimientos, así como con cualquier requisito reglamentario.
III. Supervisar periódicamente el desempeño de los proveedores para garantizar que cumplan con los requisitos de su empresa y se adhieran a sus estándares de calidad.

ELEMENTOS DEL PLAN

06 DESARROLLAR UN PLAN DE CONTINGENCIA

ORIENTACIÓN Y PASOS A SEGUIR

Desarrolle un plan de contingencia en el que se describa cómo responderá ante las interrupciones de la cadena de suministro, lo que incluye identificar proveedores alternativos y planes de respaldo adecuados para garantizar la continuidad del negocio. Para ello, deberá hacer lo siguiente:

I. Identificar los criterios para declarar una interrupción de la cadena de suministro.
II. Desarrollar procedimientos de gestión de incidentes a los que se recurrirá en caso de interrupción de la cadena de suministro.
III. Diseñar y documentar estrategias de recuperación y solución de interrupciones en la cadena de suministro.
IV. Documentar las lecciones aprendidas y los mecanismos de mejora tras las interrupciones declaradas en la cadena de suministro.

07 CAPACITAR A LOS EMPLEADOS

ORIENTACIÓN Y PASOS A SEGUIR

Capacite a sus empleados en las prácticas recomendadas de SCRM de ICT para que comprendan la importancia de gestionar los riesgos de la cadena de suministro y sus funciones en el proceso mediante las siguientes acciones:

I. Revisar los programas de capacitación vigentes para saber dónde se podría incorporar la SCRM de las ICT (por ejemplo, capacitación en adquisiciones y capacitación en seguridad).
II. Desarrollar y actualizar materiales de capacitación de empleados para incluir elementos de SCRM de ICT.
III. Identificar a las personas clave que posiblemente necesiten recibir una capacitación específica en materia de SCRM de las ICT (por ejemplo, capacitación contra la falsificación) frente a una capacitación más generalizada para toda la organización (por ejemplo, cómo adquirir bienes y servicios).

08 IMPLEMENTAR UNA SUPERVISIÓN Y MEJORA CONTINUAS

ORIENTACIÓN Y PASOS A SEGUIR

Supervise y mejore continuamente su programa de SCRM para garantizar que el contenido siga siendo eficaz y relevante para sus operaciones comerciales. Para lograrlo, debe hacer lo siguiente:

I. Supervisar a los proveedores de productos y servicios para tomar conocimiento sobre incidentes de ciberseguridad.
II. Supervisar y documentar continuamente los riesgos asociados con sus proveedores de productos y servicios.
III. Revaluar los riesgos asociados con sus proveedores de productos y servicios de forma periódica y según sea necesario.

ELEMENTOS DEL PLAN

TABLA 1: ASIGNACIÓN DE RECURSOS

Elementos del plan	Comprador	Integrador	Proveedor
1. **Empezar con un resumen ejecutivo** 2. **Identificar los riesgos de la cadena de suministro para sus activos críticos** 3. **Identificar los proveedores críticos** 4. **Contar con una diversidad de proveedores** 5. **Desarrollar un proceso de certificación de proveedores** 6. **Desarrollar un plan de contingencia** 7. **Capacitar a los empleados** 8. **Implementar una supervisión y mejora continuas**	• NIST Cybersecurity Framework Version 1.1 • NIST Special Publication 800-161R1 • NISTIR 8276 Key Practices In Cyber Supply Chain Risk Management • Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks	• NIST Cybersecurity Framework Version 1.1 • NIST Special Publication 800-161R1 • NISTIR 8276 Key Practices In Cyber Supply Chain Risk Management • Federal Acquisition Security Council Final Rule • EO 13873 Securing the ICT and Services Chain • Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks	• Federal Acquisition Security Council (FASC) Final Rule • EO 13873 Securing the ICT and Services Chain • Operationalizing the Vendor SCRM Template for Small and Medium-Sized Businesses • Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks

Los recursos incluidos en la Tabla 1 son aquellos que se utilizaron principalmente para fundamentar los elementos del plan mencionados en esta guía. Si bien los recursos se pueden aplicar a todos los elementos del plan, los recursos enumerados en las columnas respectivas son especialmente útiles si su organización se incluye en una de estas funciones. En el Apéndice A también se incluye una lista completa de recursos complementarios.

APÉNDICE A: RECURSOS COMPLEMENTARIOS

Recursos principales:

- NIST Cybersecurity Framework Version 1.1

  "El marco se centra en el uso de los factores impulsores del negocio para guiar las actividades de ciberseguridad y en la consideración de los riesgos de ciberseguridad como parte de los procesos de gestión de riesgos de la organización".

- NIST Special Publication 800-161

  El propósito de esta publicación es brindar "...orientación a las organizaciones sobre la identificación, evaluación y mitigación de los riesgos de ciberseguridad a lo largo de la cadena de suministro en todos los niveles de sus organizaciones".

- NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management

  "Este documento proporciona a la creciente comunidad de empresas digitales un conjunto de prácticas clave que cualquier organización...", independientemente de su tamaño, alcance o complejidad, "...puede utilizar para gestionar los riesgos de ciberseguridad asociados a sus cadenas de suministro".

- Federal Acquisition Security Council Final Rule

  Esta norma, que se promulgó de conformidad con la Ley de Seguridad de la Cadena de Suministro de Adquisiciones Federales (Federal Acquisition Supply Chain Security Act) de 2018, implementa "...los requisitos de las leyes que rigen el funcionamiento del Consejo Federal de Seguridad de las Adquisiciones (FASC), el intercambio de información sobre los riesgos de la cadena de suministro y la labor de las autoridades del FASC para recomendar la emisión de órdenes de remoción y exclusión con el fin de abordar los riesgos de seguridad de la cadena de suministro".

- Federal Communications Commission Covered List

  "...una lista de equipos y servicios de comunicaciones (Lista de elementos cubiertos) que se considera que representan un riesgo inaceptable para la seguridad nacional de los Estados Unidos o la seguridad y protección de los habitantes de los Estados Unidos...".

- Operationalizing the Vendor SCRM Template for Small and Medium-Sized Businesses

  Proporciona un conjunto de preguntas relativas a la implementación y aplicación por parte de un proveedor de ICT de las normas y prácticas recomendadas del sector que pueden ayudar a las pequeñas y medianas empresas a orientar la planificación de riesgos de la cadena de suministro de forma estandarizada.

- Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks

  En este manual, se proporciona una descripción general de las categorías de riesgo más altas de la cadena de suministro que comúnmente enfrentan las SMB de ICT, incluidos los riesgos cibernéticos y los recursos que pueden ayudar a las SMB.

Recursos secundarios y órdenes ejecutivas (EO):

- CISA: Secure by Design
- OMB Memorandum M-23-16
- SECURE Technology Act: Establishment of the Federal Acquisition Security Council
- Federal Acquisition Supply Chain Security Act graphic
- H.R.7327 SECURE Technology Act
- DNI ICD 731 Supply Chain Risk Management for the Intelligence Community
- DNI ICS 731-01 Supply Chain Criticality Assessment 20151002
- DNI ICS 731-02 Supply Chain Threat Assessments 20160517
- DNI ICS 731-03 Supply Chain Information Sharing

APÉNDICE A: RECURSOS COMPLEMENTARIOS

- DNI ICS 731-04 Supply Chain Vulnerability Assessments
- DNI ICS 731-05 Supply Chain Risk Assessments
- NIST: Security Measures for “EO-Critical Software” Use
- NIST: Software Supply Chain Security Guidance Under Executive Order (EO) 14028
- EO 13636 Improving Critical Infrastructure Cybersecurity
- EO 13806 Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States
- EO 13873 Securing the Information and Communications Technology and Services Supply Chain
- Executive Order 13806 Report
- EO 13913 Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector
- EO 13984 Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities
- EO 14005 Ensuring the Future Is Made in All of America by All of America’s Workers
- EO 14017 America’s Supply Chains
- EO 14024 Blocking Property with Respect to Specified Foreign Activities of the Government of the Russian Federation
- EO 14028 Improving the Nation’s Cybersecurity
- EO 14034 Protecting Americans’ Sensitive Data from Foreign Adversaries

APÉNDICE B: PARTICIPANTES COLABORADORES

Equipo directivo	Nombre	Organización
Copresidente	Ola Sage	CyberRx
Copresidente	Jeffery Goldthorp	Federal Communications Commission
Copresidente	Tamber Ray	NTCA - The Rural Broadband Association

Participantes del equipo de Redacción

Nombre	Organización
Andras Szakal	The Open Group
Bob Dix	Acquisition Advisory Council (AAC)
Chad Kliewer	ISC²
Christopher Calfee	Corporación Federal de Seguro de Depósitos (FDIC, por sus siglas en inglés)
Dick Brooks	Reliable Energy Analytics
Frank Bulk	Premier Communications
Jerry Horton	Blue Valley Technologies, Inc.
John Bienko	Administración de Pequeñas Empresas (SBA)
Justin Storms, Karen Keating	Comisión Federal de Regulación de Energía (FERC, por sus siglas en inglés)
Kathryn Basinsky, Megan Doscher	Administración Nacional de Telecomunicaciones e Información (NTIA, por sus siglas en inglés)
Larry Walke	Asociación Nacional de Radiodifusores (NAB, por sus siglas en inglés)
Leanna Wade	ActOnline
Matt Oyer	Asociación Nacional de Funcionarios de Contrataciones del Estado (NASPO, por sus siglas en inglés)
Melissa Newman	Asociación de la Industria de las Telecomunicaciones (TIA, por sus siglas en inglés)
Rebecca Adams, Briana Alston, Amanda Ingram	Agencia de Seguridad Cibernética y de Infraestructura (CISA) del Departamento de Seguridad Nacional (DHS)

PERSONA DE CONTACTO DEL DHS

Centro Nacional de Gestión de Riesgos (NMRC, por sus siglas en inglés)
Agencia de Seguridad Cibernética y de Infraestructura (CISA)
Departamento de Seguridad Nacional de EE. UU.
NRMC@hq.dhs.gov
Para obtener más información sobre NRMC, visite https://www.cisa.gov/about/divisions-offices/national-risk-management-center