Terminología de Seguridad de la Información

1. Terminología importante

El término "*Sistema de Información*" se define en U.S.C. 44, Sec. 3502 como «*un conjunto discreto de recursos de información organizados para la recopilación, procesamiento, mantenimiento, uso, intercambio, difusión o disposición de información*».

Para esta publicación, el término **sistema** se utiliza en lugar del término «*sistema de información*» para reflejar la aplicabilidad más amplia de los recursos de información de cualquier tamaño o complejidad, **organizados expresamente para la recopilación, procesamiento, uso, intercambio, difusión, mantenimiento o disposición de datos o información**. Otros términos clave que conviene conocer son[1]

- **Información** - (1) Hechos o ideas, que pueden representarse (codificarse) como diversas formas de datos; (2) Conocimiento (por ejemplo, datos, instrucciones) en cualquier medio o forma que pueda comunicarse entre entidades del sistema.
- **Seguridad de la información** - Protección de la información y los sistemas de información frente al acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados, con el fin de garantizar la confidencialidad, integridad y disponibilidad.
- **Confidencialidad** - Preservar las restricciones autorizadas de acceso y divulgación de la información, incluidos los medios para proteger la intimidad personal y la información sujeta a derechos de propiedad.
- **Integridad** - Protección contra la modificación o destrucción indebidas de la información y garantía de no repudio y autenticidad de la información.
    - **Integridad de los datos** - Propiedad de que los datos no han sido alterados de forma no autorizada. La integridad de los datos abarca los datos almacenados, durante el procesamiento y en tránsito.
    - **Integridad del sistema** - Cualidad que tiene un sistema cuando realiza su función prevista de manera intacta, libre de manipulación no autorizada del sistema, ya sea intencionada o accidental.
- **Disponibilidad** - Garantizar el acceso oportuno y fiable a la información y su utilización.
- **Controles de seguridad**[2] - Los controles de gestión, operativos y técnicos (es decir, salvaguardias o contramedidas) prescritos para un sistema con el fin de proteger la confidencialidad, disponibilidad e integridad del sistema y su información.

[1] Estos términos y definiciones fueron recuperados de CNSSI 4009, Comité de Sistemas de Seguridad Nacional (CNSS) Glosario, de fecha 6 de abril de 2015

[2] En este documento, los términos controles de seguridad, salvaguardias, protecciones de seguridad y medidas de seguridad se han utilizado indistintamente.

2. Funciones y responsabilidades

En este punto se describen las funciones específicas de la organización y sus respectivas responsabilidades. **Unas funciones y responsabilidades claramente definidas ayudan a la organización y a sus empleados a trabajar de forma más eficaz, al designar a los responsables de realizar determinadas tareas**. En una organización grande, esto ayudará a que no se pase por alto ninguna tarea. En una organización pequeña y menos estructurada, la carga de trabajo puede distribuirse de forma más uniforme, ya que un empleado puede tener que encargarse de más de una tarea.

La lista a continuación no pretende ser exhaustiva de todas las funciones posibles dentro de una organización. Cada organización puede definir sus propias funciones específicas o tener una nomenclatura diferente en función de su misión o estructura organizativa. Sin embargo, las funciones básicas siguen siendo las mismas. Para una descripción más detallada de las responsabilidades asignadas a cada función, véase NIST SP 800-37.

2.1. Función Ejecutiva de Riesgos (Alta Dirección / *Senior Management*)

La Función Ejecutiva de Riesgos es un individuo o grupo (por ejemplo, miembros del consejo, CEO, CIO) dentro de una organización responsable de asegurar que: (i) las consideraciones relacionadas con el riesgo para los sistemas individuales se ven desde una perspectiva de toda la organización, teniendo en cuenta los objetivos estratégicos generales de la organización en el desempeño de sus misiones básicas y funciones de negocio, y (ii) la gestión de los riesgos de seguridad relacionados con el sistema es coherente en toda la organización, refleja la tolerancia al riesgo de la organización, y se considera junto con otros tipos de riesgos con el fin de garantizar el éxito de la misión / negocio.

Las responsabilidades incluyen, pero no se limitan a:

- Definir un enfoque holístico para abordar los riesgos en toda la organización;
- Desarrollar una estrategia organizativa de gestión de riesgos;
- Apoyar el intercambio de información entre los responsables de la autorización y otros altos cargos de la organización.
- Supervisar las actividades relacionadas con la gestión de riesgos en toda la organización.

2.2. Director General (CEO / *Chief Executive Officer*)

El Director General es el funcionario o ejecutivo de más alto nivel en una organización con la responsabilidad general de proporcionar protecciones de seguridad de la información proporcionales al riesgo y la magnitud del daño (es decir, impacto) a los activos de las operaciones de la organización, los individuos, otras organizaciones y la Nación que pueden resultar del acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción de: (i) información recopilada o mantenida por o en nombre de la organización; y (ii) sistemas utilizados u operados por una agencia, o por un contratista de una agencia, u otra organización en nombre de una agencia.

Las responsabilidades incluyen, pero no se limitan a:

- Garantizar la integración de los procesos de gestión de la seguridad de la información con los procesos de planificación estratégica y operativa;

- Asegurarse de que la información y los sistemas utilizados para apoyar las operaciones de la organización cuentan con las salvaguardias de seguridad de la información adecuadas; y
- Confirmar que el personal formado cumple la legislación, las políticas, las directivas, las instrucciones, las normas y las directrices relacionadas con la seguridad de la información.

2.3. Director de Información (CIO / *Chief Information Officer*)

El Director de Información es un funcionario de la organización responsable de: (i) designar a un alto funcionario de seguridad de la información de la agencia; (ii) desarrollar y mantener políticas de seguridad, procedimientos y técnicas de control para abordar todos los requisitos aplicables; (iii) supervisar al personal con responsabilidades significativas para la seguridad de la información y garantizar que el personal esté adecuadamente capacitado; (iv) ayudar a los altos funcionarios de la organización con sus responsabilidades de seguridad; y (v) en coordinación con otros altos funcionarios, informar anualmente sobre la eficacia general del programa de seguridad de la información de la organización, incluido el progreso de las medidas correctivas.

Las responsabilidades incluyen, pero no se limitan a:

- Asignar recursos dedicados a la protección de los sistemas que respaldan la misión y las funciones empresariales de la organización;
- Garantizar que los sistemas están protegidos por planes de seguridad aprobados y están autorizados para funcionar.
- Asegurarse de que existe un programa de seguridad de la información para toda la organización que se aplica eficazmente.

2.4. Propietario/Administrador de la Información / *Information Owner/Steward*

El propietario/responsable de la información es un funcionario de la organización con autoridad estatutaria, de gestión u operativa para una información específica, que es responsable de establecer las políticas y procedimientos que rigen su generación, recopilación, procesamiento, difusión y eliminación.

Las responsabilidades incluyen, pero no se limitan a:

- Establecer las normas para el uso adecuado y la protección de la información en cuestión.
- Proporcionar información a los propietarios del sistema sobre los requisitos de seguridad y los controles de seguridad necesarios para proteger adecuadamente la información.

2.5. Oficial Superior de Seguridad de la Información de la Agencia (SAISO, *Senior Agency Information Security Officer*)

El Oficial Superior de Seguridad de la Información de la Agencia es un funcionario de la organización responsable de: (i) llevar a cabo las responsabilidades de seguridad del oficial principal de información bajo FISMA; y (ii) servir como el enlace principal entre el oficial principal de información y los oficiales de autorización de la organización, los propietarios del sistema, los proveedores de control común y los oficiales de seguridad del sistema. En algunas organizaciones, este papel también puede ser conocido como el Director de Seguridad de la Información (CISO).

Las responsabilidades incluyen, pero no se limitan a:

- Gestionar e implementar un programa de seguridad de la información en toda la organización; y
- Asumir el papel de representante designado oficial de autorización o evaluador de control de seguridad cuando sea necesario.

2.6. Oficial Autorizador (OA / *Authorizing Official*)

El Oficial Autorizador es un alto funcionario o ejecutivo con la autoridad para asumir formalmente la responsabilidad de operar un sistema a un nivel aceptable de riesgo para las operaciones y activos de la organización, los individuos y otras organizaciones.

Las responsabilidades incluyen, pero no se limitan a:

- Aprobar planes de seguridad, memorandos de acuerdo o entendimiento, planes de acción e hitos, así como determinar si cambios significativos en el sistema o entornos de operación requieren una nueva autorización; y
- Garantizar que los representantes designados por el funcionario autorizante lleven a cabo todas las actividades y funciones asociadas con la autorización de seguridad.

2.7. Representante designado del funcionario autorizante

El representante designado del funcionario autorizante es un funcionario de la organización que actúa en nombre de un funcionario autorizante para coordinar y llevar a cabo las actividades cotidianas requeridas asociadas al proceso de autorización de seguridad. El representante designado desempeña las funciones del OA, pero no puede asumir el riesgo del sistema.

Las responsabilidades incluyen, pero no se limitan a:

- Desempeñar las funciones del Oficial Autorizador según le sean asignadas;
- Tomar decisiones con respecto a la planificación y dotación de recursos del proceso de autorización de seguridad, la aprobación del plan de seguridad, la aprobación y supervisión de la aplicación de planes de acción e hitos, y la evaluación y/o determinación del riesgo; y
- Preparar el paquete de autorización final, obtener la firma del funcionario autorizante en el documento de decisión de autorización, y transmitir el paquete de autorización a los funcionarios apropiados de la organización.

2.8. Alto Funcionario de la Agencia para la Privacidad (SAOP / *Senior Agency Official for Privacy*)

El Alto Funcionario de la Agencia para la Privacidad es un alto funcionario de la organización que tiene la responsabilidad general de garantizar la aplicación por parte de la agencia de las protecciones de la privacidad de la información, incluido el pleno cumplimiento por parte de la agencia de las leyes, reglamentos y políticas federales relativas a la privacidad de la información, como la Ley de Privacidad.

Sus responsabilidades incluyen, entre otras, las siguientes

- Supervisar, coordinar y facilitar los esfuerzos de cumplimiento de la privacidad de la agencia;

- Revisar los procedimientos de privacidad de la información de la agencia para garantizar que son exhaustivos y están actualizados; y
- Garantizar que los empleados y contratistas de la agencia reciban los programas de formación y educación adecuados en relación con las leyes, reglamentos, políticas y procedimientos de privacidad de la información que rigen el tratamiento de la información personal por parte de la agencia.

2.9. Proveedor de controles comunes

El proveedor de controles comunes es una persona, grupo u organización responsable del desarrollo, la aplicación, la evaluación y la supervisión de los controles comunes (es decir, los controles de seguridad heredados por los sistemas).

Sus responsabilidades incluyen, pero no se limitan a:

- Documentar los controles comunes identificados por la organización en un plan de seguridad (o documento equivalente prescrito por la organización); y
- Garantizar que las evaluaciones requeridas de los controles comunes son llevadas a cabo por evaluadores cualificados con un nivel adecuado de independencia definido por la organización.

2.10. Propietario del sistema

El propietario del sistema es un funcionario de la organización responsable de la adquisición, desarrollo, integración, modificación, operación, mantenimiento y eliminación de un sistema.

Sus responsabilidades incluyen, entre otras, las siguientes:

- Abordar los intereses operativos de la comunidad de usuarios (es decir, los usuarios que requieren acceso al sistema para satisfacer los requisitos de la misión, del negocio u operativos);
- Garantizar el cumplimiento de los requisitos de seguridad de la información.
- Desarrollar y mantener el plan de seguridad del sistema y garantizar que el sistema se despliega y opera de acuerdo con los controles de seguridad acordados.

2.11. Responsable de seguridad del sistema (SSO / *System Security Officer*)

El Responsable de Seguridad del Sistema es responsable de garantizar que se mantenga una postura de seguridad operativa adecuada para un sistema y, como tal, trabaja en estrecha colaboración con el propietario del sistema.

Sus responsabilidades incluyen, entre otras, las siguientes:

- Supervisar las operaciones diarias de seguridad de un sistema.
- Asistir en el desarrollo de las políticas y procedimientos de seguridad y garantizar el cumplimiento de dichas políticas y procedimientos.

2.12. Arquitecto de Seguridad de la Información / *Information Security Architect*

El Arquitecto de Seguridad de la Información es un individuo, grupo u organización responsable de asegurar que los requerimientos de seguridad de la información necesarios para proteger las misiones centrales de la organización y los procesos de negocio sean adecuadamente tratados en todos los aspectos de la arquitectura empresarial, incluyendo modelos de referencia, modelos de segmentos y soluciones, y los sistemas resultantes que soportan esas misiones y procesos de negocio.

Las responsabilidades incluyen, pero no se limitan a:

- Servir de enlace entre el arquitecto de la empresa y el ingeniero de seguridad de la información.
- Coordinar con los propietarios del sistema, los proveedores de controles comunes y los responsables de seguridad del sistema la asignación de controles de seguridad como controles específicos del sistema, híbridos o comunes.

2.13. Ingeniero de Seguridad de Sistemas (SSE / *System Security Engineer*)

El Ingeniero de Seguridad de Sistemas es un individuo, grupo u organización responsable de llevar a cabo actividades de ingeniería de seguridad de sistemas.

Las responsabilidades incluyen, pero no se limitan a:

- Diseñar y desarrollar sistemas organizativos o actualizar sistemas heredados; y
- Coordinar las actividades relacionadas con la seguridad con arquitectos de seguridad de la información, oficiales superiores de seguridad de la información de la agencia, propietarios del sistema, proveedores de control común y oficiales de seguridad del sistema.

2.14. Evaluador del control de seguridad / *Security Control Assessor*

El evaluador de controles de seguridad es un individuo, grupo u organización responsable de llevar a cabo una evaluación exhaustiva de los controles de seguridad técnicos, operativos y de gestión, así como de las mejoras de control empleadas dentro de un sistema o heredadas por éste, para determinar la eficacia general de los controles (es decir, el grado en que los controles se aplican correctamente, funcionan según lo previsto y producen el resultado deseado con respecto al cumplimiento de los requisitos de seguridad del sistema).

Las responsabilidades incluyen, entre otras, las siguientes:

- Proporcionar una evaluación para identificar debilidades o deficiencias en el sistema y su entorno de operación;
- Recomendar medidas correctivas para abordar las vulnerabilidades identificadas; y
- Preparar un informe de evaluación de la seguridad que contenga los resultados y conclusiones de la evaluación.

2.15. Administrador del sistema

El Administrador del Sistema es un individuo, grupo u organización responsable de configurar y mantener un sistema o componentes específicos de un sistema.

Las responsabilidades incluyen, pero no se limitan a:

- Instalación, configuración y actualización de hardware y software;
- Establecer y gestionar cuentas de usuario;
- Supervisar las tareas de copia de seguridad y recuperación.
- Implantar controles técnicos de seguridad.

2.16. Usuario

El Usuario es un individuo, grupo u organización al que se le concede acceso a la información de la organización para realizar las tareas asignadas.

Las responsabilidades incluyen, pero no se limitan a:

- Adherirse a las políticas que rigen el uso aceptable de los sistemas de la organización;
- Utilizar los recursos informáticos proporcionados por la organización únicamente para los fines definidos.
- Informar de anomalías o comportamientos sospechosos del sistema.

2.17. Funciones de apoyo / *Supporting Roles*

- **Auditor**: Los auditores son responsables de examinar los sistemas para determinar: (i) si el sistema cumple los requisitos de seguridad establecidos y las políticas de la organización; y (ii) si los controles de seguridad son apropiados. Las auditorías informales pueden ser realizadas por aquellos que operan el sistema bajo revisión o por auditores terceros imparciales.
- **Personal de seguridad física** / *Physical Security Staff*. La oficina de seguridad física es responsable de desarrollar y hacer cumplir los controles de seguridad física apropiados, a menudo en consulta con la gestión de la seguridad de la información, los directores de programas y funcionales, y otros. La seguridad física se ocupa de las instalaciones del sistema central, las instalaciones de respaldo y los entornos de oficina. En el gobierno, esta oficina es a menudo responsable de procesar los controles de antecedentes del personal y las autorizaciones de seguridad.
- **Personal de recuperación en caso de catástrofe/planes de contingencia** / *Disaster Recovery/Contingency Planning Staff*. Algunas organizaciones cuentan con personal independiente para la recuperación en caso de catástrofe y la planificación de contingencias. En tales casos, el personal suele ser responsable de la planificación de contingencias para toda la organización y trabaja con los directores de programas y funcionales/propietarios de aplicaciones, el personal de seguridad de la información y otros para obtener apoyo adicional de planificación de contingencias, según sea necesario.

- **Personal de garantía de calidad** / *Quality Assurance Staff*. Muchas organizaciones han establecido un programa de garantía de calidad para mejorar los productos y servicios que ofrecen a sus clientes. El personal de garantía de calidad debe tener conocimientos prácticos de seguridad de la información y de cómo puede utilizarse para mejorar la calidad del programa (por ejemplo, garantizando la integridad de la información informática, la disponibilidad de los servicios y la confidencialidad de la información de los clientes).

- **Personal de la oficina de adquisiciones** / *Procurement Office Staff*. La oficina de compras (o adquisiciones) es responsable de garantizar que las adquisiciones de la organización han sido revisadas por los funcionarios adecuados. Aunque el personal de la oficina de adquisiciones carece de los conocimientos técnicos necesarios para garantizar que los bienes y servicios cumplen las expectativas de seguridad de la información, debe, no obstante, conocer las normas de seguridad de la información y señalar los posibles problemas de seguridad de la información a quienes solicitan dicha tecnología.

- **Formación del personal de la oficina** / *Training Office Staff*. La organización determina si la responsabilidad principal de la formación de usuarios, operadores y gestores en materia de seguridad de la información recae en la oficina de formación o en la oficina del programa de seguridad de la información. En cualquier caso, las dos organizaciones deben trabajar juntas para desarrollar un programa de formación eficaz.

- **Recursos Humanos** / *Human Resources*. La oficina de Recursos Humanos suele ser el primer punto de contacto para los directivos que necesitan ayuda para determinar si es necesaria o no una investigación de antecedentes de seguridad para un puesto concreto. Las oficinas de recursos humanos y de seguridad suelen colaborar estrechamente en cuestiones relacionadas con las investigaciones de antecedentes. La oficina de recursos humanos también puede ser responsable de los procedimientos de salida relacionados con la seguridad cuando los empleados abandonan una organización.

- **Personal de gestión/planificación de riesgos** / *Risk Management/Planning Staff*. Algunas organizaciones emplean personal a tiempo completo dedicado a analizar todo tipo de riesgos a los que puede estar expuesta la organización. Aunque esta oficina normalmente se centra en cuestiones de riesgos organizativos, también debe considerar los riesgos relacionados con la seguridad de la información. Esta oficina no suele realizar análisis de riesgos para sistemas específicos.

- **Personal de planta física** / *Physical Plant Staff*. Esta oficina es responsable de garantizar la prestación de los servicios necesarios para el funcionamiento seguro de los sistemas de una organización (por ejemplo, energía eléctrica y controles ambientales). A menudo, la oficina cuenta con personal médico, de bomberos, de residuos peligrosos o de seguridad.

- **Personal de la Oficina de Privacidad** / *Privacy Office Staff*. Esta oficina es responsable de mantener un programa integral de privacidad que garantice el cumplimiento de los requisitos de privacidad aplicables, desarrolle y evalúe la política de privacidad y gestione los riesgos de privacidad. Esta oficina incluye un alto funcionario autorizado para la privacidad, especialistas en cumplimiento de la privacidad y evaluación de riesgos, especialistas jurídicos y otros profesionales centrados en la gestión de los riesgos para la privacidad, y en particular

3. Amenazas y vulnerabilidades: Un breve resumen

Una **vulnerabilidad** es una debilidad en un sistema, procedimiento de seguridad del sistema, controles internos o implementación que podría ser explotada por una **fuente de amenaza**[3]. Las vulnerabilidades dejan los sistemas susceptibles a una multitud de actividades que pueden resultar en pérdidas significativas y a veces irreversibles para un individuo, grupo u organización. Estas pérdidas pueden ir desde un único archivo dañado en un ordenador portátil o dispositivo móvil hasta bases de datos enteras en un centro de operaciones que se vean comprometidas. Con las herramientas y los conocimientos adecuados, un adversario puede explotar las vulnerabilidades de los sistemas y acceder a la información almacenada en ellos. El daño infligido a los sistemas comprometidos puede variar en función del origen de la amenaza.

Una fuente de amenaza puede ser adversaria o no adversaria. **Las fuentes de amenazas adversarias** son individuos, grupos, organizaciones o entidades que buscan explotar la dependencia de una organización de los recursos cibernéticos. Incluso empleados, usuarios privilegiados y usuarios de confianza han sido conocidos por defraudar los sistemas organizativos. **Las fuentes de amenazas no adversarias** se refieren a desastres naturales o acciones erróneas llevadas a cabo por individuos en el curso de la ejecución de sus responsabilidades diarias.

Si el sistema es vulnerable, las fuentes de amenaza pueden conducir a **eventos de amenaza**. Un evento de amenaza es un incidente o situación que potencialmente podría causar consecuencias o impactos no deseados. Un ejemplo de una fuente de amenaza que conduce a un evento de amenaza es un hacker que instala un monitor de pulsaciones de teclas en un sistema de la organización. Los daños que los eventos de amenaza pueden causar en los sistemas varían considerablemente. Algunos afectan a la confidencialidad e integridad de la información almacenada en un sistema, mientras que otros sólo afectan a la disponibilidad del sistema. Para más información sobre fuentes de amenazas y eventos de amenazas, véase NIST SP 800-30.

Este capítulo presenta una visión general del entorno en el que operan los sistemas hoy en día y puede resultar valioso para las organizaciones que buscan una mejor comprensión del entorno de amenazas específico. La lista que aquí se ofrece no pretende ser exhaustiva. El alcance de la información aquí proporcionada puede ser demasiado amplio, y las amenazas contra sistemas específicos podrían ser muy diferentes de lo que se discute en este capítulo.

Para proteger un sistema del riesgo e implementar las medidas de seguridad más rentables, los propietarios, administradores y usuarios del sistema necesitan conocer y comprender las vulnerabilidades del sistema, así como las fuentes de amenazas y los eventos que pueden explotar las vulnerabilidades. Al determinar la respuesta apropiada a una vulnerabilidad descubierta, se debe tener cuidado de minimizar el gasto de recursos en vulnerabilidades donde hay poca o ninguna amenaza presente. La *Gestión de Riesgos de Seguridad de la Información*, trata sobre cómo se relacionan las amenazas, las vulnerabilidades, la selección de salvaguardas y la respuesta al riesgo.

3.1. Ejemplos de fuentes y eventos de amenazas adversarias

En la sección anterior se definieron las fuentes de amenaza y los eventos de amenaza. Esta sección proporciona varios ejemplos de cada uno de ellos, seguidos de una descripción.

[3] Fuente de amenaza - La intención y el método dirigido a la explotación intencional de una vulnerabilidad o una situación y método que puede explotar accidentalmente una vulnerabilidad

3.1.1. Fraude y robo

Los sistemas pueden ser explotados para cometer fraudes y robos «automatizando» los métodos tradicionales de fraude o utilizando nuevos métodos. El fraude y el robo de sistemas pueden ser cometidos por personas internas (es decir, usuarios autorizados) y externas. Los administradores autorizados del sistema y los usuarios con acceso y familiaridad con el sistema (por ejemplo, los recursos que controla, los fallos) suelen ser responsables de fraude. Los antiguos empleados de una organización también suponen una amenaza, dado su conocimiento de las operaciones de la organización, sobre todo si el acceso no se interrumpe con prontitud.

El beneficio económico es una de las principales motivaciones del fraude y el robo, pero los sistemas financieros no son los únicos que corren peligro. Existen varias técnicas que un individuo puede utilizar para obtener información a la que de otro modo no habría tenido acceso. Algunas de estas técnicas son

- **Redes sociales**. La ubicuidad de las redes sociales (por ejemplo, Facebook, Twitter, LinkedIn) ha permitido a los ciberdelincuentes explotar la plataforma para llevar a cabo ataques selectivos. Utilizando cuentas de redes sociales falsas, fáciles de crear y no verificadas, los ciberdelincuentes pueden hacerse pasar por compañeros de trabajo, representantes de atención al cliente u otras personas de confianza para enviar enlaces a códigos maliciosos que roban información personal o confidencial de la organización. Las redes sociales agravan el actual problema del fraude, y las organizaciones deben considerarlo una seria preocupación a la hora de implantar sistemas. Las cuentas de las redes sociales proporcionan un medio para recopilar información de contacto, intereses y conexiones personales de un individuo objetivo que, a su vez, puede utilizarse para llevar a cabo un ataque de ingeniería social.
- **Ingeniería social**. La ingeniería social, en el contexto de la seguridad de la información, es una técnica que se basa en gran medida en la interacción humana para influir en una persona a fin de que viole el protocolo de seguridad y la anime a divulgar información confidencial. Este tipo de ataques se cometen habitualmente por teléfono o en línea. Los ataques perpetrados por teléfono son los ataques de ingeniería social más básicos que se cometen. Por ejemplo, un atacante puede engañar a una empresa haciéndole creer que el atacante es un cliente existente y hacer que la empresa divulgue información sobre ese cliente. En Internet, esta técnica se denomina phishing, un ataque basado en el correo electrónico que pretende engañar a las personas para que realicen una acción beneficiosa para el atacante (por ejemplo, hacer clic en un enlace o divulgar información personal). Los ataques de ingeniería social en línea también pueden llevarse a cabo mediante el uso de archivos adjuntos que contienen código malicioso, cuyo objetivo es la libreta de direcciones de una persona. La información obtenida permite al atacante enviar código malicioso a todos los contactos de la libreta de direcciones de la víctima, propagando el daño del ataque inicial.
- **Amenaza persistente avanzada** (**APT**). Una amenaza persistente avanzada es una intrusión a largo plazo que intenta acceder a datos e información específicos. En lugar de intentar causar daños, los ataques APT están diseñados para recopilar información de la red o del objetivo. Algunos ataques APT pueden ser tan complicados que, para no ser detectados por los sistemas de detección de intrusos (IDS) de la red, requieren que un administrador reescriba el código las 24 horas del día. Una vez recopilada suficiente información sobre la red, el atacante puede crear una puerta trasera, que es una forma de eludir los mecanismos de seguridad de los sistemas, y acceder a la red sin ser detectado. A continuación, el atacante utiliza un sistema externo de mando y control para vigilar continuamente el sistema y extraer información.

3.1.2. Amenaza interna

Los empleados pueden representar una amenaza interna para una organización dada su familiaridad con los sistemas y aplicaciones del empleador, así como con las acciones que pueden causar más daños, travesuras o desórdenes. El sabotaje de los empleados -a menudo instigado por el conocimiento o la amenaza de despido- es un problema crítico para las organizaciones y sus sistemas. En un esfuerzo por mitigar el daño potencial causado por el sabotaje del empleado, el acceso del empleado despedido a la infraestructura de TI debe ser inmediatamente desactivado, y el individuo debe ser escoltado fuera de las instalaciones de la empresa.

Ejemplos de sabotaje de empleados relacionados con el sistema incluyen, pero no se limitan a:

- Destrucción de hardware o instalaciones;
- Introducir código malicioso que destruya programas o datos;
- Introducir datos incorrectamente, retener datos o borrar datos;
- Bloqueo de sistemas; y
- Cambiar las contraseñas administrativas para impedir el acceso al sistema.

3.1.3. Hacker malintencionado

Hacker malicioso es un término usado para describir a un individuo o grupo que usa su conocimiento de sistemas, redes y programación para acceder ilegalmente a sistemas, causar daño o robar información. Comprender la motivación que impulsa a un hacker malicioso puede ayudar a una organización a implementar los controles de seguridad adecuados para evitar la probabilidad de una violación del sistema.

El hacker malicioso es una amplia categoría de amenazas adversas que puede dividirse en categorías más pequeñas dependiendo de las acciones específicas o la intención del hacker malicioso. Algunas de las subcategorías adaptadas de NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*, incluyen:

- **Atacantes** / *Attackers*. Los atacantes irrumpen en las redes por la emoción y el desafío o para presumir en la comunidad de atacantes. Mientras que antes la piratería remota requería considerables habilidades o conocimientos informáticos, ahora los atacantes pueden descargar secuencias de comandos y protocolos de ataque de Internet y lanzarlos contra los sitios de las víctimas. Estas herramientas de ataque se han vuelto más sofisticadas y más fáciles de usar. En algunos casos, los atacantes carecen de los conocimientos necesarios para amenazar objetivos difíciles, como las redes gubernamentales críticas. No obstante, la población mundial de atacantes plantea una amenaza relativamente alta de interrupciones aisladas o breves que podrían causar graves daños a empresas o infraestructuras.
- **Operadores de redes de bots** / *Bot-Network Operators*. Los operadores de redes de bots asumen el control de múltiples sistemas para coordinar ataques y distribuir esquemas de phishing, spam y código malicioso. Los servicios de sistemas y redes comprometidos pueden encontrarse en mercados clandestinos en línea (por ejemplo, comprando un ataque de denegación de servicio, utilizando servidores para retransmitir spam o ataques de phishing).
- **Grupos delictivos** / *Criminal Groups*. Los grupos delictivos intentan atacar sistemas para obtener beneficios económicos. En concreto, los grupos delictivos organizados utilizan el spam,

el phishing y el spyware/código malicioso para cometer robos de identidad y fraudes en línea. Los espías corporativos internacionales y las organizaciones del crimen organizado también suponen una amenaza para la nación debido a su capacidad para llevar a cabo espionaje industrial, robos monetarios a gran escala y el reclutamiento de nuevos atacantes. Algunos grupos delictivos pueden intentar extorsionar a una organización amenazándola con un ciberataque o cifrando e interrumpiendo sus sistemas a cambio de un rescate. Los ataques de extorsión o rescate han perturbado numerosas empresas y su mitigación ha costado importantes recursos y planificación. Sin planes de copia de seguridad y procedimientos de restauración eficaces, muchas empresas han recurrido al pago de costosos rescates para restaurar sus sistemas cifrados.

- **Servicios de inteligencia extranjeros** / *Foreign Intelligence Services*. Los servicios de inteligencia extranjeros utilizan herramientas cibernéticas como parte de sus actividades de recopilación de información y espionaje. Además, varias naciones están trabajando enérgicamente para desarrollar doctrinas, programas y capacidades de guerra de la información. Estas capacidades permiten que una sola entidad tenga un impacto significativo y grave al interrumpir las infraestructuras de suministro, comunicaciones y económicas que sustentan el poder militar, impactos que podrían afectar a la vida cotidiana de los ciudadanos estadounidenses.

  En algunos casos, pueden estar presentes amenazas planteadas por servicios de inteligencia de gobiernos extranjeros. Además del posible espionaje económico, los servicios de inteligencia extranjeros pueden apuntar a sistemas no clasificados para promover sus misiones de inteligencia. Alguna información no clasificada que puede ser de interés incluye planes de viaje de altos funcionarios, defensa civil y preparación para emergencias, tecnologías de fabricación, datos de satélites, datos de personal y nóminas, y archivos de aplicación de la ley, investigación y seguridad.

- **Phishers**. Los *phishers* son individuos o pequeños grupos que ejecutan esquemas de phishing para robar identidades o información con fines lucrativos. Los phishers también pueden utilizar spam y spyware/código malicioso para lograr sus objetivos.

- **Spammers**. Los *spammers* son individuos u organizaciones que distribuyen correo electrónico no solicitado con información oculta o falsa para vender productos, llevar a cabo esquemas de phishing, distribuir spyware/código malicioso o atacar organizaciones (por ejemplo, DoS).

- **Autores de spyware/código malicioso**. Individuos u organizaciones que maliciosamente llevan a cabo ataques contra usuarios produciendo y distribuyendo spyware y código malicioso. Entre los virus y gusanos informáticos destructivos que han dañado archivos y discos duros se incluyen el macrovirus Melissa, el gusano Explore.Zip, el virus CIH (Chernobyl), Nimda, Code Red, Slammer y Blaster.

- **Terroristas** / *Terrorists*. Los terroristas intentan destruir, incapacitar o explotar infraestructuras críticas para amenazar la seguridad nacional, causar víctimas masivas, debilitar la economía de Estados Unidos y dañar la moral y la confianza del público. Los terroristas pueden utilizar esquemas de phishing o spyware/código malicioso para generar fondos o recabar información sensible. También pueden atacar un objetivo para desviar la atención o los recursos de otros objetivos.

- **Espionaje industrial** / *Industrial Spies*. El espionaje industrial busca adquirir propiedad intelectual y conocimientos técnicos utilizando métodos clandestinos.

3.1.4. Código malicioso

Código malicioso se refiere a virus, troyanos, gusanos, bombas lógicas y cualquier otro software creado con el propósito de atacar una plataforma.

- **Virus**. Segmento de código que se replica adjuntando copias de sí mismo a ejecutables existentes. La nueva copia del virus se ejecuta cuando un usuario ejecuta el nuevo programa anfitrión. El virus puede incluir una «carga útil» adicional que se activa cuando se cumplen determinadas condiciones.
- **Caballo de Troya** / *Trojan Horse*. Programa que realiza una tarea deseada, pero que también incluye funciones inesperadas e indeseables. Por ejemplo, considere un programa de edición para un sistema multiusuario. Este programa podría modificarse para borrar de forma aleatoria e inesperada los archivos de un usuario cada vez que realiza una función útil (por ejemplo, editar).
- **Gusano** / *Worm.*. Programa autorreplicante que es autónomo y no requiere un programa anfitrión ni la intervención del usuario. Los gusanos suelen utilizar servicios de red para propagarse a otros sistemas anfitriones.
- **Bomba lógica** / **Logic Bomb**. Este tipo de código malicioso es un conjunto de instrucciones insertadas secreta e intencionadamente en un programa o sistema de software para llevar a cabo una función maliciosa en una fecha y hora predispuestas o cuando se cumple una condición específica.
- **Ransomware**. Es un tipo de código malicioso que bloquea o limita el acceso a un sistema bloqueando toda la pantalla o bloqueando o cifrando archivos específicos hasta que se paga un rescate. Hay dos tipos diferentes de ataques de ransomware: los encriptadores y los bloqueadores. Los **encriptadores o cifradores** bloquean (cifran) los archivos del sistema y exigen un pago para desbloquearlos (o descifrarlos). Los cifradores, o cripto-ransomware, son los más comunes y preocupantes (por ejemplo, WannaCry). Los **bloqueadores** están diseñados para bloquear a los usuarios de los sistemas operativos. El usuario sigue teniendo acceso al dispositivo y a otros archivos, pero para desbloquear el ordenador infectado se le pide que pague un rescate. Para empeorar las cosas, incluso si el usuario paga el rescate, no hay garantía de que el atacante realmente proporcione la clave de descifrado o desbloquee el sistema infectado.

3.2. Ejemplos de fuentes y eventos de amenaza no adversarial

3.2.1. Errores y omisiones

Los errores y omisiones pueden ser causados inadvertidamente por operadores de sistemas que procesan cientos de transacciones diariamente o por usuarios que crean y editan datos en sistemas organizacionales. Estos errores y omisiones pueden degradar la integridad de los datos y del sistema. Las aplicaciones informáticas, independientemente de su nivel de sofisticación, no son capaces de detectar todos los tipos de errores y omisiones de entrada.

Por lo tanto, es responsabilidad de la organización establecer un sólido programa de concienciación y formación para reducir el número y la gravedad de los errores y omisiones.

Los errores cometidos por los usuarios, los operadores del sistema o los programadores pueden producirse a lo largo del ciclo de vida de un sistema y contribuir directa o indirectamente a los problemas de seguridad. En algunos casos, el error es una amenaza, como un error de entrada de

datos o un error de programación que bloquea un sistema. En otros casos, los errores causan vulnerabilidades. Los errores de programación y desarrollo, a menudo denominados «bugs», pueden ser desde benignos hasta catastróficos.

3.2.2. Pérdida de soporte físico y de infraestructura

La pérdida de infraestructuras de apoyo incluye cortes de electricidad (por ejemplo, apagones, picos, caídas de tensión), pérdida de comunicaciones, cortes y fugas de agua, averías en el alcantarillado, interrupción de los servicios de transporte, incendios, inundaciones, disturbios civiles y huelgas. La pérdida de infraestructuras de apoyo suele provocar paradas inesperadas del sistema. Por ejemplo, es posible que los empleados no puedan ir a trabajar durante una tormenta invernal, aunque los sistemas del lugar de trabajo funcionen con normalidad.

3.2.3. Efectos del intercambio de información sobre la intimidad personal

La acumulación de grandes cantidades de información de identificación personal por parte de organizaciones gubernamentales y privadas ha creado numerosas oportunidades para que los individuos experimenten problemas de privacidad como subproducto o consecuencia involuntaria de una violación de la seguridad. Por ejemplo, la migración de información a un proveedor de servicios en la nube se ha convertido en una opción viable que muchas personas y organizaciones utilizan. La facilidad de acceso a los datos desde la nube la ha convertido en una solución más atractiva para el almacenamiento a largo plazo. Todo lo que se escribe, se carga o se publica se almacena en un sistema en la nube que los individuos no controlan. Sin embargo, sin que lo sepa el usuario del servicio en la nube, un extraño con las herramientas y los conocimientos técnicos adecuados puede acceder a la información personal.

El hecho de que las personas compartan voluntariamente información personal a través de las redes sociales también ha contribuido a la aparición de nuevas amenazas que permiten a piratas informáticos malintencionados utilizar esa información con fines de ingeniería social o para eludir las medidas de autenticación habituales. Uniendo toda esta información y tecnología, los hackers malintencionados tienen la capacidad de crear cuentas utilizando la información de otra persona u obtener acceso a las redes.

Las organizaciones pueden compartir información sobre ciberamenazas que incluya IPI. Estas divulgaciones podrían dar lugar a usos imprevistos de dicha información, incluida la vigilancia u otras acciones policiales.

4. Política de seguridad de la información

El término **política** tiene más de una definición cuando se habla de seguridad de la información. NIST SP 800-95, Guide to Secure Web Services, define política como «*declaraciones, reglas o afirmaciones que especifican el comportamiento correcto o esperado de una entidad*». Por ejemplo, una política de autorización podría especificar las reglas correctas de control de acceso para un componente de software. El término política también puede referirse a reglas de seguridad específicas para un sistema o incluso a las decisiones de gestión específicas que dictan la política de privacidad del correo electrónico o la política de seguridad de acceso remoto de una organización.

La política de seguridad de la información se define como un conjunto de directivas, reglamentos, normas y prácticas que prescriben cómo una organización gestiona, protege y distribuye la información. Al tomar estas decisiones, los directivos se enfrentan a decisiones difíciles con res-

pecto a la asignación de recursos, los objetivos en competencia y la estrategia organizativa, todo ello relacionado con la protección de los recursos técnicos y de información, así como con la orientación del comportamiento de los empleados. Los directivos de todos los niveles toman decisiones que pueden afectar a la política, y el alcance de la aplicabilidad de la política varía en función del ámbito de autoridad del directivo.

Las decisiones de los directivos en materia de seguridad de la información son muy variadas. Para diferenciar los distintos tipos de políticas, este capítulo las clasifica en tres tipos básicos: Política de Programa, Política de Asunto Específico, y Política de Sistema Específico.

Los controles de política son abordados por los controles «-1» para cada familia de control de seguridad que se encuentran en el NIST SP 800-53. Los controles «-1» establecen la política y los procedimientos para la aplicación efectiva del control de seguridad y la mejora de control seleccionados.

4.1. Normas, directrices y procedimientos

Dado que la política se escribe a un nivel amplio, las organizaciones también desarrollan normas, directrices y procedimientos que ofrecen a los usuarios, gerentes, administradores de sistemas y otros un enfoque más claro para implementar la política y cumplir con los objetivos de la organización. Las normas y directrices especifican las tecnologías y metodologías que deben utilizarse para proteger los sistemas. Los procedimientos son pasos más detallados que deben seguirse para llevar a cabo tareas relacionadas con la seguridad. Las normas, directrices y procedimientos pueden promulgarse en toda la organización a través de manuales, reglamentos o instrucciones.

- Los **estándares organizativos** (que no deben confundirse con los Estándares Nacionales Americanos, FIPS, Estándares Federales u otros estándares nacionales o internacionales) especifican el uso uniforme de tecnologías, parámetros o procedimientos específicos cuando dicho uso uniforme beneficie a una organización. Un ejemplo típico es la normalización de las tarjetas de identificación en toda la organización, que facilita la movilidad de los empleados y la automatización de los sistemas de entrada y salida. Las normas suelen ser obligatorias dentro de una organización.
- Las **directrices** ayudan a los usuarios, al personal de sistemas y a otras personas a proteger eficazmente sus sistemas. La naturaleza de las directrices, sin embargo, reconoce inmediatamente que los sistemas varían considerablemente, y la imposición de normas no siempre es factible, apropiada o rentable. Por ejemplo, una directriz organizativa puede utilizarse para ayudar a desarrollar procedimientos estándar específicos del sistema. Las directrices se utilizan a menudo para ayudar a garantizar que no se pasan por alto medidas de seguridad específicas, aunque pueden aplicarse, y correctamente, de más de una manera.
- Los **procedimientos** describen cómo poner en práctica las políticas, normas y directrices de seguridad aplicables. Son pasos detallados que deben seguir los usuarios, el personal de operaciones del sistema u otras personas para realizar una tarea concreta (por ejemplo, preparar nuevas cuentas de usuario y asignar los privilegios adecuados).

Algunas organizaciones publican manuales, reglamentos, manuales o documentos similares sobre seguridad de la información en general. En ellos se pueden mezclar políticas, directrices, normas y procedimientos, ya que están estrechamente relacionados. Aunque los manuales y reglamentos pueden servir como herramientas importantes, a menudo es útil que distingan claramente entre la política y su aplicación. Esto puede ayudar a promover la flexibilidad y la rentabilidad al ofrecer enfoques de aplicación alternativos para alcanzar los objetivos políticos.

4.2. Política de programas

La política del programa se utiliza para crear el programa de seguridad de la información de una organización. Las políticas de programa establecen la dirección estratégica para la seguridad y asignan recursos para su implementación dentro de la organización. Un funcionario de la gerencia -típicamente el SISO- emite la política del programa para establecer o reestructurar el programa de seguridad de la información de la organización. Esta política de alto nivel define el propósito del programa y su alcance dentro de la organización, aborda cuestiones de cumplimiento y asigna responsabilidades a la organización de seguridad de la información para la implementación directa del programa, así como otras responsabilidades relacionadas.

4.2.1. Componentes básicos de la política del programa

La política del programa aborda los siguientes aspectos:

- **Propósito**. La política del programa a menudo incluye una declaración que describe el propósito y las metas del programa. Las necesidades relacionadas con la seguridad tales como integridad, disponibilidad y confidencialidad pueden formar la base de las metas organizacionales establecidas en la política. Por ejemplo, en una organización responsable del mantenimiento de grandes bases de datos de misión crítica, se podría hacer hincapié específicamente en la reducción de errores, pérdida de datos, corrupción de datos y recuperación. Sin embargo, en una organización responsable del mantenimiento de datos personales confidenciales, los objetivos podrían hacer hincapié en una mayor protección contra la divulgación no autorizada.
- **Alcance**. Las políticas del programa son claras en cuanto a qué recursos (por ejemplo, instalaciones, hardware y software, información y personal) protege el programa de seguridad de la información. En muchos casos, el programa abarcará todos los sistemas y el personal de la organización, mientras que en otros, puede ser apropiado que el programa de seguridad de la información de una organización tenga un alcance más limitado. Por ejemplo, una política destinada a proteger la información almacenada en un sistema clasificado o de alto impacto será mucho más estricta que la de una política destinada a asegurar un sistema considerado de bajo impacto.
- **Responsabilidades**. Una vez establecido el programa de seguridad de la información, su gestión se asigna normalmente a una oficina de nueva creación o ya existente. También es necesario abordar las responsabilidades de los funcionarios y oficinas de toda la organización. Esta sección de la declaración de política, por ejemplo, distinguiría entre las responsabilidades de los proveedores de servicios de información y los gestores de las aplicaciones que utilizan los servicios proporcionados. La política también establecería oficinas de seguridad operativa para los principales sistemas, en particular los de alto riesgo o los más críticos para las operaciones de la organización. También puede servir como base para establecer la responsabilidad de los empleados.
- **Cumplimiento**. La política del programa suele abordar dos cuestiones de cumplimiento:

    1. Cumplimiento general para garantizar el cumplimiento de los requisitos para establecer un programa y las responsabilidades asignadas en el mismo a los distintos componentes de la organización. A menudo se asigna a una entidad de supervisión (por ejemplo, el Inspector General) la responsabilidad de supervisar el cumplimiento, incluido el grado en que la organización está aplicando las prioridades de la dirección para el programa.

2. El uso de sanciones y acciones disciplinarias específicas. Dado que la política de seguridad es un documento de alto nivel, normalmente no se detallan aquí las sanciones específicas para las distintas infracciones. En su lugar, la política puede autorizar la creación de estructuras de cumplimiento que incluyan infracciones y acciones disciplinarias específicas.

Un aspecto importante de la elaboración de la política de cumplimiento es recordar que la infracción de la política por parte de un empleado puede ser involuntaria. Por ejemplo, el incumplimiento puede ser a menudo el resultado de una falta de conocimientos o de formación. La necesidad de obtener orientación de un asesor jurídico adecuado es fundamental a la hora de abordar cuestiones relacionadas con sanciones y medidas disciplinarias para las personas. No es necesario que la política reitere sanciones ya contempladas por la ley, aunque pueden enumerarse si la política también se utilizará como documento de concienciación o formación.

4.3. Política específica

Basándose en las orientaciones de la política de seguridad de la información, se desarrollan políticas específicas para abordar áreas de relevancia y preocupación actuales para una organización. La intención es proporcionar orientación específica e instrucciones sobre el uso adecuado de los sistemas a los empleados dentro de la organización. Una política específica se aplica a todas las tecnologías que utiliza la organización y se redacta de forma que resulte clara para los usuarios. A diferencia de las políticas de programa, las políticas específicas deben revisarse periódicamente debido a los frecuentes cambios tecnológicos de una organización.

4.3.1. Ejemplos de temas para una política específica

Hay muchas áreas para las que puede ser apropiada una política específica. Las nuevas tecnologías y el descubrimiento de nuevas amenazas requieren a menudo la creación de una política específica. Algunos ejemplos de políticas específicas son:

- **Acceso a Internet**. Conectarse a Internet conlleva muchas ventajas, pero también muchos problemas. Algunas de las cuestiones que puede abordar una política de acceso a Internet son la identificación de quién tendrá acceso, qué tipos de sistemas pueden conectarse a la red, qué tipos de información pueden transmitirse a través de la red, los requisitos de autenticación de usuarios para los sistemas conectados a Internet y el uso de cortafuegos.
- **Privacidad del correo electrónico**. Esta política aclarará qué información se recopila y almacena y el uso que se hace de ella. Es posible que la dirección desee supervisar al empleado para asegurarse de que sólo utiliza los sistemas de la organización con fines empresariales, o para determinar si el empleado está distribuyendo virus, enviando contenidos ofensivos o revelando información empresarial privada. A los usuarios se les puede conceder un cierto nivel de privacidad en relación con el correo electrónico, y esta política aborda qué nivel de privacidad esperar, así como las circunstancias en las que el correo electrónico puede ser leído.
- **Traiga su propio dispositivo (BYOD, *Bring Your Own Device*)**. Permite a las personas utilizar dispositivos personales en el lugar de trabajo. Permitir BYOD puede aumentar la productividad y reducir los costes para la organización. Sin embargo, introducir diferentes sistemas operativos y configuraciones de usuario en la red de la organización puede suponer un reto, no sólo para la seguridad de la información de la organización, sino también para

la privacidad del empleado. Una política BYOD completa tiene consideraciones específicas para el dispositivo y el usuario, así como normas de comportamiento que deben cumplirse para acceder a los recursos de la organización utilizando dispositivos personales.

- **Redes sociales**. Aunque la organización no tenga presencia en las redes sociales, lo más probable es que sus usuarios sí la tengan. Tener una política de redes sociales es crucial para proteger a la organización y a sus empleados. Una política de medios sociales proporciona directrices para los usuarios que delinean el comportamiento esperado al utilizar diferentes plataformas de medios sociales. Dependiendo de la organización, la política puede ser estricta -no permitir el uso de los medios sociales en los recursos proporcionados por la organización- o una política indulgente que permita el acceso a los medios sociales dentro de las limitaciones especificadas por la organización.

Otros temas que pueden ser objeto de una política específica son, entre otros: el enfoque de la gestión de riesgos y los planes de contingencia, la protección de la información confidencial/de propiedad, el software no autorizado, el uso no autorizado de equipos, las infracciones de la política, el uso de almacenamiento externo, los derechos de privacidad y las emergencias físicas.

4.3.2. Componentes básicos de la política temática

Una política específica puede dividirse en los siguientes componentes:

- **Enunciado de la cuestión**. Para formular una política sobre una cuestión, el propietario/responsable de la información debe definir primero la cuestión e incluir todos los términos, distinciones y condiciones pertinentes. A menudo resulta útil especificar el objetivo o la justificación de la política para facilitar su cumplimiento. Por ejemplo, una organización podría querer desarrollar una política específica sobre el uso de «software no oficial», que podría definirse como cualquier software no aprobado, adquirido, controlado, gestionado o propiedad de la organización. Además, podría ser necesario incluir las distinciones y condiciones aplicables para algunos programas informáticos, como los de propiedad privada de los empleados pero aprobados para su uso en el trabajo, o los de propiedad y uso de otras empresas contratadas por la organización.
- **Declaración de la posición de la organización**. Una vez planteada la cuestión y detallados los términos y condiciones relacionados, esta sección se utiliza para exponer claramente la posición de la organización (es decir, la decisión de la dirección) al respecto. Según el ejemplo anterior, esto significaría indicar si el uso de software no oficial, tal y como se ha definido, está prohibido en todos o en algunos casos, si existen directrices adicionales para la aprobación y el uso, o si se pueden conceder excepciones caso por caso, por quién y sobre qué base.
- **Aplicabilidad**. Las políticas temáticas también deben incluir declaraciones de aplicabilidad. Esto significa aclarar dónde, cómo, cuándo, a quién y a qué se aplica una política. Por ejemplo, podría ser que la política hipotética sobre software no oficial sólo se aplicara a los recursos y empleados de la propia organización y no a los contratistas con oficinas en otros lugares. Además, podría ser necesario aclarar la aplicabilidad de la política en lo que respecta a los empleados que viajan entre distintas sedes, que trabajan desde casa o que necesitan transportar y utilizar discos en varias sedes.
- **Funciones y responsabilidades**. La asignación de funciones y responsabilidades también suele incluirse en las políticas específicas. Por ejemplo, si la política permite a los empleados utilizar software privado no oficial en el trabajo con las aprobaciones pertinentes, habría que

indicar la autoridad que concede dicho permiso. (Del mismo modo, habría que aclarar quién sería responsable de garantizar que sólo se utilice software aprobado en los recursos del sistema de la organización y, posiblemente, de supervisar a los usuarios en relación con el software no oficial.

- **Cumplimiento**. Para algunos tipos de política, puede ser conveniente describir con mayor detalle las infracciones inaceptables y las consecuencias de dicho comportamiento. Las sanciones pueden establecerse explícitamente y ser coherentes con las políticas y prácticas de personal de la organización. Cuando se utilicen, pueden coordinarse con los funcionarios, oficinas e incluso unidades de negociación de los empleados que corresponda. También puede ser conveniente encargar a una oficina específica de la organización la supervisión del cumplimiento.

- **Puntos de contacto e información complementaria**. Para cualquier política específica, indique las personas de la organización con las que debe ponerse en contacto para obtener más información, orientación y cumplimiento. Dado que los cargos tienden a cambiar con menos frecuencia que las personas que los ocupan, puede ser preferible utilizar cargos específicos como punto de contacto. Por ejemplo, para algunas cuestiones, el punto de contacto podría ser un superior jerárquico; para otras, podría ser un responsable de las instalaciones, una persona de asistencia técnica, un administrador de sistemas o un representante del programa de seguridad. Utilizando de nuevo el ejemplo anterior, los empleados necesitarían saber si el punto de contacto para preguntas e información sobre procedimientos sería su superior inmediato, un administrador de sistemas o un funcionario de seguridad de la información.

4.4. Política específica del sistema

Las políticas específicas de programa y asunto son políticas amplias y de alto nivel escritas para abarcar toda la organización, mientras que las políticas específicas de sistema proporcionan información y dirección sobre qué acciones están permitidas en un sistema en particular. Estas políticas son similares a las políticas específicas de un problema en el sentido de que se refieren a tecnologías específicas de toda la organización. Sin embargo, las políticas específicas del sistema dictan las configuraciones de seguridad apropiadas al personal responsable de implementar los controles de seguridad requeridos para satisfacer las necesidades de seguridad de la información de la organización.

Para desarrollar un conjunto cohesivo y completo de políticas de seguridad, los responsables pueden utilizar un proceso de gestión que derive las normas de seguridad de los objetivos de seguridad. Resulta útil considerar un modelo de dos niveles para la política de seguridad del sistema: objetivos de seguridad y normas de seguridad operativa.

Sin embargo, la aplicación de la política en la tecnología está estrechamente vinculada y a menudo es difícil de distinguir. De forma similar a las políticas específicas de cada asunto, se recomienda que las políticas específicas de cada sistema se revisen según lo requiera el periodo de tiempo definido por la organización para garantizar su conformidad con los procedimientos de seguridad más actuales.

4.4.1. Objetivos de seguridad

El primer paso en el proceso de gestión es definir objetivos de seguridad proporcionales al riesgo para el sistema específico. Aunque este proceso puede comenzar con un análisis de la necesidad de integridad, confidencialidad y disponibilidad, no puede detenerse ahí. Un objetivo

de seguridad tiene que ser específico, concreto, bien definido y enunciado de tal manera que sea un objetivo claramente alcanzable. Las partes interesadas desempeñan un papel importante en el desarrollo de una política global, pero práctica. Por lo tanto, es imperativo recordar que la política no la crea únicamente el personal directivo.

4.4.2. Normas de seguridad operativa

Después de que la dirección determine los objetivos de seguridad, se pueden identificar y documentar las reglas para gestionar y operar un sistema. Por ejemplo, las reglas pueden definir las modificaciones autorizadas - especificando los individuos autorizados a tomar ciertas acciones bajo condiciones particulares con respecto a clases específicas y registros de información. El grado de especificidad necesario para la seguridad operativa varía de un sistema a otro. Cuanto más detalladas sean las normas, más fácil será para los administradores determinar cuándo se ha producido una infracción. Una descripción detallada también puede agilizar la automatización de la aplicación de las políticas.

Además de decidir el nivel de detalle, la dirección determina el grado de formalidad de la documentación de la política específica del sistema. Una vez más, cuanto más formal sea la documentación, más fácil será aplicar y seguir la política. Por ejemplo, una práctica útil sería redactar una declaración de los privilegios de acceso a un sistema, así como la asignación de responsabilidades de seguridad. También deben abordarse las normas de uso del sistema y las consecuencias de su incumplimiento. La documentación de la política de control de acceso puede facilitar considerablemente su seguimiento y aplicación.

Las decisiones políticas en otras áreas de la seguridad de la información, como las descritas en esta publicación, suelen documentarse en el análisis de riesgos, las declaraciones de acreditación o los manuales de procedimiento. Sin embargo, cualquier política controvertida, atípica o poco común también necesitará declaraciones formales. Las políticas atípicas pueden incluir áreas en las que la política del sistema varía de la política de la organización o de la práctica normal dentro de la organización. La documentación de una política típica contiene una declaración que explica la razón de la desviación de la política estándar de la organización.

4.4.3. Aplicación de políticas específicas del sistema

La tecnología desempeña un papel importante en la aplicación de políticas específicas del sistema, pero no es la única responsable de satisfacer las necesidades de seguridad de una organización. Cuando se utiliza la tecnología para hacer cumplir las políticas, es importante tener en cuenta los métodos manuales. Por ejemplo, podrían utilizarse controles técnicos basados en el sistema para limitar la impresión de informes confidenciales a una impresora específica. Sin embargo, también habría que aplicar las correspondientes medidas de seguridad física para limitar el acceso a la salida de la impresora o no se lograría el objetivo de seguridad deseado.

Los métodos tecnológicos utilizados con frecuencia para aplicar la política de seguridad del sistema incluyen probablemente el uso de controles de acceso lógicos. Algunos ejemplos de controles de acceso serían: la separación de funciones, que es un control diseñado para abordar el potencial de abuso de los privilegios autorizados y ayuda a reducir el riesgo de actividad malintencionada sin colusión; y el privilegio mínimo, que sólo permite el acceso autorizado a los usuarios o procesos que actúan en nombre de los usuarios que es necesario para realizar las tareas asignadas de acuerdo con las misiones de la organización y las funciones empresariales.

Sin embargo, existen otros medios automatizados para aplicar o respaldar la política de seguridad que suelen complementar los controles de acceso lógicos. Por ejemplo, el software de

detección de intrusos puede alertar a los administradores del sistema de actividades sospechosas o incluso tomar medidas para detenerlas.

La aplicación de la política de seguridad del sistema basada en la tecnología tiene ventajas e inconvenientes. Un sistema, correctamente diseñado, programado, instalado, configurado y mantenido, hace cumplir de forma coherente la política dentro del sistema, aunque ningún sistema puede obligar a los usuarios a seguir todos los procedimientos. Los controles de gestión también desempeñan un papel importante en la aplicación de la política, por lo que descuidarlos sería perjudicial para la organización. Además, las desviaciones de la política pueden ser a veces necesarias y apropiadas; estas desviaciones pueden ser difíciles de implementar fácilmente con algunos controles técnicos. Esta situación se produce con frecuencia si la aplicación de la política de seguridad es demasiado rígida, lo que puede ocurrir cuando los analistas de sistemas no prevén las contingencias y no se preparan para ellas.

4.5. Interdependencias

La política está relacionada con muchos de los temas tratados en esta publicación:

- **Gestión de programas**. La política se utiliza para establecer el programa de seguridad de la información de una organización y por lo tanto está estrechamente ligada a la gestión y administración del programa. Tanto el programa como la política específica del sistema pueden establecerse en cualquiera de las áreas cubiertas en esta publicación. Por ejemplo, una organización puede desear tener un enfoque consistente para la planificación de contingencia para todos sus sistemas y emitiría una política de programa apropiada para hacerlo. Por otro lado, puede decidir que sus sistemas son lo suficientemente independientes entre sí como para que los propietarios de los sistemas puedan hacer frente a los incidentes de forma individual.
- **Controles de acceso**. La política específica del sistema se implementa a menudo utilizando controles de acceso. Por ejemplo, puede ser una decisión política que sólo dos individuos en una organización estén autorizados a ejecutar un programa de impresión de cheques. Los controles de acceso son utilizados por el sistema para implementar o hacer cumplir esta política.
- **Vínculos con políticas organizativas más amplias**. Es importante entender que las políticas de seguridad de la información son a menudo extensiones de otras políticas organizativas. El apoyo y la coordinación deben ser recíprocos entre la seguridad de la información y otras políticas organizativas para minimizar la confusión. Por ejemplo, la política de correo electrónico de una organización probablemente sea relevante para su política más amplia sobre privacidad.

4.6. Consideraciones sobre los costes

El desarrollo e implementación de políticas de seguridad de la información conlleva una serie de costes potenciales. Los costes más significativos son la implementación de la política y el tratamiento de sus impactos subsiguientes en la organización, sus recursos y su personal. El establecimiento de un programa de seguridad de la información, logrado a través de la política, probablemente no tenga un coste insignificante.

Otros costes pueden ser los derivados del proceso de desarrollo de la política. Pueden ser necesarias numerosas actividades administrativas y de gestión para redactar, revisar, coordinar, aprobar, difundir y publicar las políticas. En muchas organizaciones, la aplicación satisfactoria de

las políticas puede requerir personal y formación adicionales. En general, los costes que supone para una organización la elaboración y aplicación de una política de seguridad de la información dependerán de la amplitud que deba tener el cambio para que la dirección decida que se ha alcanzado un nivel de riesgo aceptable.

El coste de proteger la información y los sistemas es inevitable. El objetivo es garantizar que las protecciones de seguridad sean proporcionales al riesgo, estableciendo un equilibrio entre las protecciones necesarias para cumplir los objetivos de seguridad de la organización y el coste de dichas protecciones.