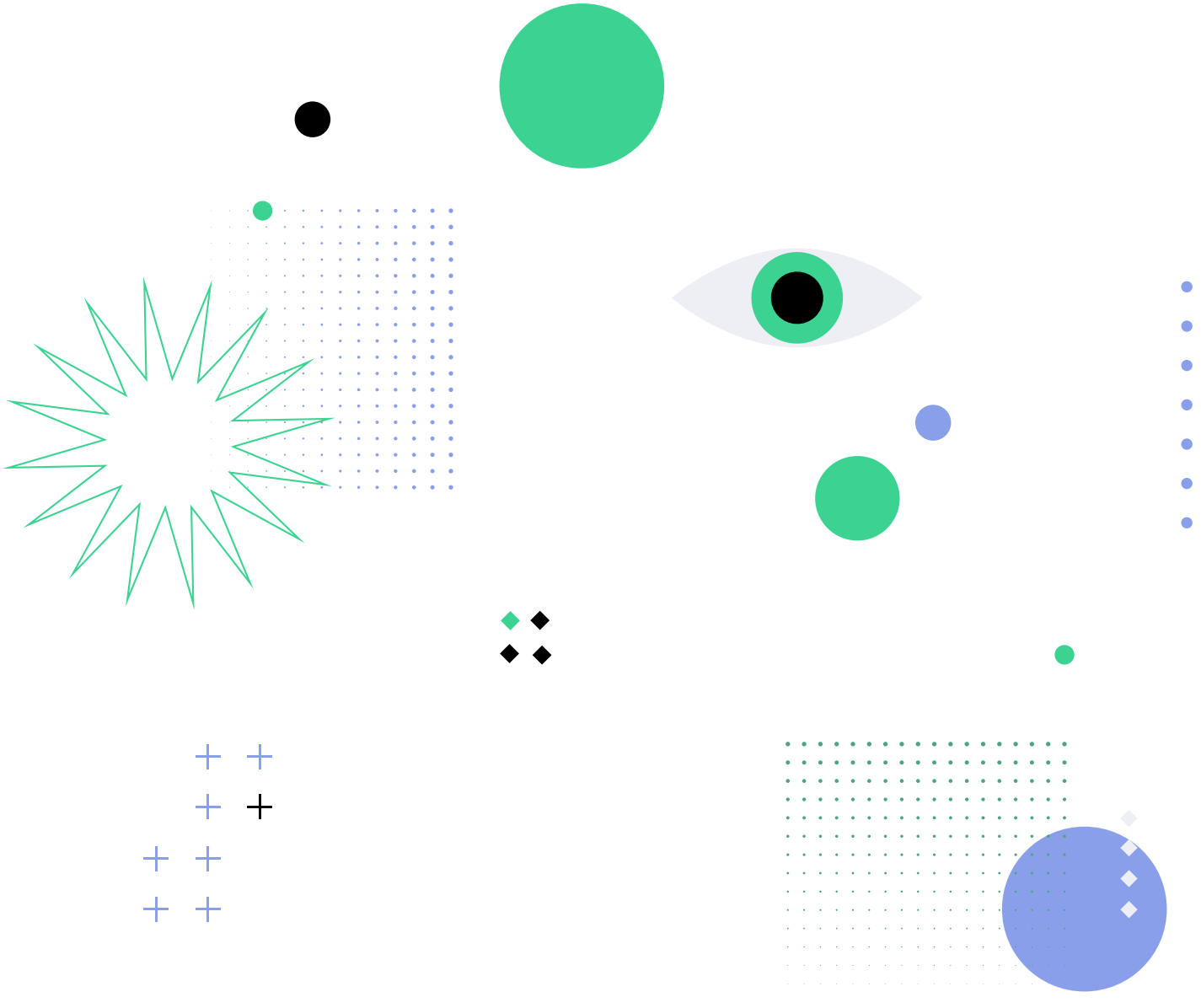
FUNDACIONSADOSKY.ORG.AR

Seguridad de la información y ciberseguridad



Fundación SADOSKY

Ministerio de Ciencia, Tecnología e Innovación
Argentina

Seguridad de la información y ciberseguridad

Autoría

Marcela Pallero
Directora del área de Seguridad TIC de la Fundación Sadosky

Juan Martín Heguiabehere
Seguridad TIC, Fundación Sadosky

Colaboración

Agustina Brizio
Subsecretaria de Tecnologías de la Información

Olga Cavalli
Directora Nacional de Ciberseguridad

Diseño Gráfico

Jaqueline Schaab
Fundación Sadosky

Autoridades de la Fundación Dr. Manuel Sadosky

Daniel Filmus
Presidente

Fernando Schapachnik
Director Ejecutivo

Índice

Introducción

¿Cuál es la finalidad del documento?

Este documento tiene como finalidad brindar un aporte al debate público en torno a la problemática de los incidentes que afectan a empresas, organismos públicos y a la ciudadanía en general para el desarrollo de políticas públicas relacionadas con la ciberseguridad. Este debate se extiende desde los aspectos más técnicos hacia los efectos que producen en las sociedades y su transversalidad institucional.

Ante la creciente complejidad y dependencia tecnológica de las organizaciones actuales, se vuelve cada vez más prioritaria la inclusión de las prácticas recomendadas por los estándares nacionales e internacionales reconocidos en materia de seguridad de la información.

Además, la protección de la información propia de las organizaciones, el cuidado de los servicios que se brindan a las personas usuarias, clientes y clientas, así como la protección de los datos personales, son objetivos que hoy se vuelven estratégicos. En tanto que si se ven afectados por un incidente grave que no haya sido previsto puede implicar, tanto para empresas como organismos públicos, interrupciones críticas del funcionamiento, pérdida de confianza o de reputación.

De esta manera, la implementación de un marco de gestión de seguridad de la información en la amplitud de las actividades que comprende aún no es habitual en las organizaciones del país y se debe impulsar desde todos los ámbitos.

Este documento tiene un lenguaje sencillo y está destinado a cualquier persona que se interese en la seguridad de la información y aquello que se entiende por ciberseguridad.

¿A quién está dirigido?

Los alcances de los temas de seguridad informática son técnicos y pueden ser muy complejos. Se habla de las campañas de concientización para que las personas tengan cuidado con sus contraseñas y también están las medidas organizativas y técnicas que suelen pedir las regulaciones de protección de datos, la necesidad de tener un presupuesto asignado a la seguridad de la información y su implementación a partir de una gestión de riesgos.

En este contexto, el primer paso es entender a qué nos referimos con los distintos términos. Luego diferenciarlos, explicarlos y conocer los principales estándares internacionales en la materia como referencias. Estas diferencias conceptuales pueden ser cruciales al momento de asignar responsabilidades y de implementar alguna de las prácticas en una empresa u organismo público. También es importante al momento de leer una norma regulatoria o al redactarla. La seguridad de la información está presente en normas regulatorias de historias clínicas, de temas financieros, etc.

Estas disciplinas son nuevas respecto de las más tradicionales y los tecnicismos y diversos usos de los términos no están consensuados para el público en general y generan confusiones.

La seguridad de la información es importante en la gestión de cualquier tipo de industria o servicios; es relevante para garantizar derechos fundamentales y en tanto la ciudadanía

está obligada a brindar sus datos personales al Estado, también lo será como instrumento en su protección.

Por la complejidad que suponen los aspectos técnicos y la relevancia que representa para la sociedad, se presenta a continuación un conjunto de explicaciones como breve acercamiento de utilidad en la dirección y la gestión de las organizaciones en la actualidad, así como a sus integrantes y público estudiante en general.

¿A qué se llama Seguridad de la información?

Se denomina seguridad de la información al conjunto de prácticas destinadas a preservar la integridad, la disponibilidad y la confidencialidad de la información con independencia de su soporte y desde el punto de vista de procesos. La visión de la seguridad de la información se integra a las distintas funciones de una organización para incluir las prácticas recomendadas, tanto en los procesos de la organización como en sus servicios. Por esta razón, se debe tener conocimiento de la misión y funciones de la organización, así como de las prácticas y estándares de la seguridad de la información para poder integrarlas de manera completa.

La Gestión de la seguridad de la información incluye el diseño e implementación de planes de prevención desde los distintos procesos (clasificación de la información, gestión de accesos, de vulnerabilidades y amenazas, evaluación de riesgos, etc.) que se relacionan dentro de la organización, la gestión de los recursos necesarios para dichas actividades, y la consideración de un análisis de riesgos que permita balancear objetivos de seguridad con recursos disponibles y la exposición a las amenazas con mayor probabilidad de afectar a la organización.

Adicionalmente, en el contexto de una organización pública o privada, la asignación de responsabilidades debe ser clara para una correcta rendición de cuentas, tanto para la gestión operativa como para las posibles consecuencias administrativas o judiciales ante incidentes.

En este sentido, los procedimientos de mayor relevancia deberán estar documentados para evidenciar los análisis y la aprobación de las autoridades.

¿Es lo mismo seguridad de la información que seguridad informática?

La seguridad informática es una disciplina técnica que contempla las medidas de seguridad aplicadas en el ámbito de la tecnología informática y de telecomunicaciones, ya sea el desarrollo de sistemas de información, los protocolos de comunicación, aplicaciones móviles, las infraestructuras, las bases de datos, la virtualización, las "nubes", las redes, los dispositivos que incluyen un circuito integrado, etc. De manera genérica, comprende la seguridad del software, del hardware, de las redes y de sus interacciones.

En ciertos contextos se utilizan de manera indistinta. Sin embargo, es mejor entender las diferencias, describir las funciones y alcances de la manera más precisa posible.

Por otro lado, en general, cuando se menciona seguridad de la información se incluye a la seguridad informática. En este contexto, resulta relevante asegurarse que los alcances de los términos que se utilizan sean los correctos.

En grandes líneas, las personas expertas en seguridad informática tienen conocimientos y habilidades en técnicas en desarrollo seguro, técnicas de hacking, aseguramiento de redes, administración de sistemas, configuraciones seguras (hardening) o análisis de malware, por mencionar las más requeridas.

En el caso de la seguridad de la información, el conocimiento y habilidades están dados por el campo de implementación de buenas prácticas para la gestión de la seguridad de manera transversal e integral en una organización, es decir, los distintos estándares y procesos, la definición de planes, normas y procedimientos y su implementación, así como su vinculación con la gestión de los riesgos de las tecnologías de la información.

La implementación de medidas técnicas de seguridad para el software, el hardware y las redes constituyen actividades básicas que se estructurarán y organizarán en función de los procesos y sus actividades. En el mismo sentido, los procesos deben administrarse de manera continua, para adecuarse a los cambios.

Las organizaciones cambian cuando incorporan o rotan sus empleados, cuando adquieren o actualizan el equipamiento informático, cuando se desarrollan nuevos sistemas de información o aplicaciones y todo tipo de redes, así como cuando se materializan cambios en las funciones o en los productos. Por estos motivos se deben realizar los mantenimientos y actualizaciones necesarias de manera planificada, diseñar y establecer planes de respuesta ante incidentes y participar en el diseño e implementación de los planes de resiliencia.

Para las organizaciones que adoptan el modelo de gestión de servicios de Tecnologías de la Información o TI (ITIL[1] o ISO/IEC 20000), tanto de manera interna como en los servicios que brindan a la ciudadanía, los aspectos de seguridad forman parte del ciclo de vida de dichos servicios, desde su diseño hasta su finalización. Además, la implementación de seguridad debe incorporarse en los niveles de operación, gestión y hasta en la dirección.

1 ITIL es un conjunto de buenas prácticas para la mejora de los servicios de Tecnologías de la información

¿Qué es la gestión del riesgo? ¿Qué tipo de riesgos son de interés para la seguridad de la información?

La gestión del riesgo es un proceso que parte de analizar la probabilidad de que ocurran ciertos eventos y los impactos que pueden causar. Hay estándares que, de manera general, lo definen como una medida de la incertidumbre.

Los riesgos que son de interés de la seguridad de la información son los derivados de eventos que afectan a la integridad, disponibilidad y confidencialidad de la información, a los sistemas de información y a las redes, así como a la organización y a las personas en tanto recursos humanos de la organización.

En particular, también deberán analizarse los riesgos cuando un proceso que originalmente se realizaba en papel o de manera presencial se convierta en digital o utilice tecnología.

Por otro lado, hay una gran cantidad de otros riesgos que debería contemplar una organización, como los riesgos reputacionales ante un incidente o los de incumplimiento legal respecto a las regulaciones, estatutos internos y normas aplicables a la misión y función de la organización.

Para gestionar los riesgos es muy importante entender cuáles son los activos a proteger, cuáles son las amenazas y las vulnerabilidades que pueden tener las tecnologías y los procesos; así como el rol y actividades de las personas. Por esta razón, en las etapas iniciales, una de las actividades principales es la identificación y evaluación de los riesgos, en particular aquellos que afectan a los activos de mayor criticidad o importancia para la organización, independientemente de la metodología a utilizar.

GRÁFICO 1. **ELEMENTOS DEL RIESGO**

Dependiendo del tamaño y complejidad de una organización, tal vez sea necesario implementar un marco de referencia que contemple todos los riesgos que puedan afectarla.

¿Qué entendemos por gestión de incidentes de seguridad de la información?

Los incidentes de seguridad de la información son eventos que afectan a la integridad, disponibilidad y confidencialidad de la información o a los sistemas de información o sus servicios. También son incidentes la transgresión de políticas de seguridad o de uso aceptable de recursos informáticos, independientemente de si hubo intención o no de causar daño por parte de la entidad que lo originó.

La gestión de incidentes en el contexto de una organización es el ciclo de preparación y atención durante sus distintas etapas y el aprendizaje posterior. Se puede considerar un proceso que se vincula tanto a los aspectos de análisis del riesgo de seguridad de la información como al monitoreo de los controles, su operación y mantenimiento.

GRÁFICO 2. **ETAPAS GENÉRICAS DE LA GESTIÓN DE INCIDENTES**

La gestión de los incidentes debe ser analizada desde sus distintas etapas y documentada en un Plan de Respuesta ante incidentes. Este plan, en términos generales, comprende las siguientes etapas: detección, registro, priorización, análisis que permita determinar posibles impactos, evaluación para escalar el tratamiento y activar el plan o planes de continuidad del negocio, contención para que el incidente no escale o se propague, recuperación para restablecer servicios y, finalmente, la etapa de lecciones aprendidas.

En esta línea deberá analizarse y estudiarse el caso particular en el que el incidente afecte a datos personales, ya sea de clientes y clientas en caso de empresas, datos de personas usuarias o empleadas de la organización, para incluir las buenas prácticas y regulación en la materia.

En un Plan de Respuesta ante incidentes, además, también deben contemplarse las posibles y necesarias estrategias de comunicación tanto interna como de cara al público. En este sentido, y dependiendo del tamaño y complejidad de la organización, debe coordinarse con otras áreas, como prensa o relaciones institucionales.

¿Qué son los controles? y ¿los objetivos de control?

En este contexto, los controles o medidas de seguridad son actividades que permiten modificar el riesgo. A fin de minimizarlo, los controles se implementan como medidas preventivas, detectivas, correctivas o disuasivas.

Las preventivas tienen como fin evitar la ocurrencia de eventos de seguridad. Las medidas detectivas son aquellas que tienen como objetivo, que una vez iniciado un evento que no pudo prevenirse, este sea detectado. Los controles correctivos minimizan o contienen los impactos negativos, una vez que un incidente ocurre, y los disuasivos se disponen para alejar a quien practique un ataque o desincentivar alguna conducta en particular.

Los controles tienen también un ciclo de vida: comenzando por el diseño, la implementación, la evaluación de su efectividad y las posibilidades de mejora o actualización ante cambios o una evaluación negativa.

Los controles preventivos son los más eficientes, en tanto su objetivo puede ser minimizar la posibilidad de ocurrencia o impacto antes de que tenga lugar un evento no deseado .

Un “objetivo de control” es un estado o situación que se desea obtener, es decir, una meta a alcanzar. Este resultado se puede lograr con la aplicación de uno o varios controles.

En el marco de la seguridad de la información, las normas de alto nivel pueden describirse en términos de objetivos de control, ya que deberían establecer requisitos independientes de las tecnologías y de las implementaciones.

Una situación en particular que puede ser ejemplo de un objetivo de control es: “que las organizaciones puedan realizar trazabilidad de sus operaciones”, entonces para cumplir con ese objetivo, las organizaciones pueden implementar controles técnicos, como pueden ser la habilitación de logs o registros de auditoría de sus sistemas, la documentación y el procedimiento de la asignación de las personas usuarias a los sistemas con la capacitación sobre el uso de los sistemas y las implicancias sobre el uso de sus credenciales.

PREVENTIVOS	**DETECTIVOS**	**CORRECTIVOS**
Controles destinados a prevenir o evitar incidentes de seguridad de la información, antes de la ocurrencia de un incidente.	Controles destinados a detectar, es decir, durante la ocurrencia de un incidente de seguridad de la información, reduciendo o mitigandio el impacto.	Controles destinados a contener o mitigar impactos una vez que el incidente de seguridad de la información ocurrió.

GRÁFICO 3. **TIPOS DE CONTROLES**

¿Cuál es la relación con la gestión de las tecnologías y la gestión de los datos?

La gestión de las tecnologías, en este contexto, refiere a la administración de las adquisiciones, el mantenimiento, las actualizaciones, los cambios, las adaptaciones, reposición, desactivación, destrucción, desarrollo de software, de la infraestructura, los servicios y los sistemas de información en todo su ciclo de vida. La gestión de los datos, por otro lado, refiere al ciclo de tratamiento de los datos desde la recolección hasta su uso o procesamiento, cesión o transferencia, o eliminación, para lograr el mayor aporte de valor a la organización.

Una consideración no menor es que la gestión de la seguridad de la información debe estar coordinada con la gestión de las TIC (de sistemas, de infraestructuras, comunicaciones, etc.) o como se denomine al área en la organización pública o privada.

Una de las actividades centrales para la gestión del riesgo y de la seguridad de la información se basa en la identificación y clasificación del dato o la información, así como de los procesos, el software, el hardware y las actividades de las personas, para priorizar la asignación de recursos en la protección de activos y servicios de mayor valor para la organización.

En este sentido, la gestión de la seguridad de la información, desde el análisis del riesgo, la protección de datos y la gestión de las tecnologías, son áreas y funciones de trabajo que cuando la organización pública o privada diseña sus propios servicios digitales, debería ver en su conjunto. Es decir, incorporar a los requerimientos funcionales, los requisitos de seguridad y privacidad desde el diseño.

Por las razones mencionadas en la implementación de servicios, a través de sistemas de información o aplicaciones en que se da tratamiento a los datos personales, deberán observarse tanto los aspectos de tecnología como los de seguridad, protección de datos personales y privacidad.

GRÁFICO 4. **ELEMENTOS PARA LA GESTIÓN DEL RIESGO DE CIBERSEGURIDAD**

¿Cómo se relaciona la seguridad de la información con el tratamiento de datos personales?

Expresado el objetivo general de la gestión del dato, cuando éste además corresponde a la categoría de dato personal, su tratamiento deberá circunscribirse a los principios reglamentados por ley. En Argentina se encuentra vigente a la fecha la Ley Nro. 25326 que contiene los siguientes requerimientos:

CONSENTIMIENTO

El tratamiento de datos personales es lícito cuando el titular presta su consentimiento libre, expreso e informado, que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo con las circunstancias.

En este sentido, la Ley 25326 en Argentina exime de la necesidad del consentimiento cuando se recaben para el ejercicio de funciones propias de los Poderes del Estado o en virtud de una obligación legal.

FINALIDAD O LIMITACIÓN DE PROPÓSITO

Los datos personales se recolectan con un propósito. Para ese objetivo se obtiene el consentimiento y no pueden utilizarse para otros fines.

MINIMIZACIÓN DEL DATO

Los datos recolectados deben ser estrictamente los necesarios para la finalidad requerida y ninguno más.

CONFIDENCIALIDAD

Se obliga al secreto profesional a quienes tienen acceso a datos personales durante el tratamiento.

EXACTITUD

Desde la protección del dato personal, la exactitud en el tratamiento resguarda que el dato sea completo y se encuentre actualizado de manera tal que la persona titular pueda validarlo.

SEGURIDAD DEL DATO

La ley argentina 25326, en su artículo 9 expresa que la persona responsable o usuaria del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales.

En términos de nuestra legislación nacional, el o la Responsable de archivo, registro, base o banco de datos es la persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

Cabe mencionar que en la terminología de Protección de datos personales, se denomina tratamiento a las operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y, en general, el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Adicionalmente, se debe mencionar que para el cumplimiento con el principio de seguridad de los datos personales es necesario la implementación de un conjunto de medidas técnicas y organizativas. Estas medidas son las mencionadas a lo largo de este documento como controles de seguridad de la información. De esta manera se vincula la Protección de datos personales y la seguridad de la información.

¿Cómo se puede abordar la Seguridad de la Información en una organización?

Las propiedades de la seguridad de la información

Las propiedades son características que tomadas como objetivos para determinado dato, información o servicio debieran asegurarse mediante controles. Los controles podrán ser preventivos, detectivos o correctivos, y también pueden ser tanto técnicos como administrativos u organizacionales.

Los controles técnicos se materializan o concretan a través de software o hardware y los controles organizativos o administrativos pueden ser normas, políticas o procedimientos, así como estructuras orgánicas o unidades administrativas.

La seguridad de la información se define por sus propiedades básicas, la confidencialidad, integridad y disponibilidad, y también por algunas más que podrían ser requeridas, como la autenticidad, la responsabilidad demostrada (accountability), no repudio, protección a la duplicación y confiabilidad. A continuación, se brindan unas breves descripciones.

CONFIDENCIALIDAD

La confidencialidad resguarda que la información no esté disponible o sea accedida o divulgada a individuos, entidades o procesos que no cuenten con una autorización. Esta propiedad es la que definida como objetivo para un tipo de información en particular, protege a los datos y la información a través de distintos tipos de controles. En conjunto con el principio de “necesidad de saber” que indica que la persona empleada o agente público sólo debería acceder a aquella información que es necesaria para realizar su tareas asignadas, brindan desde el punto de vista de seguridad de la información, una meta necesaria.

INTEGRIDAD

La integridad resguarda la exactitud y totalidad de la información. El objetivo de proteger la integridad de la información es que no pueda ser modificada o que al ser modificada, pueda detectarse. Incluye también protección contra la creación y la eliminación de datos sin autorización.

DISPONIBILIDAD

La disponibilidad es la propiedad de la información para asegurar que esté accesible y sea utilizable en el momento que se la requiera por una entidad autorizada. En este sentido, los controles técnicos y administrativos deberán tener estos objetivos. Los procedimientos, software y planificación de resguardos y copias de seguridad están dirigidos a asegurar la disponibilidad de información, la capacidad de brindar servicio cuando se lo requiera o ante incidentes.

AUTENTICIDAD

La autenticidad busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se busca asegurar el origen de la información, validando el emisor para evitar suplantación de identidades.

ACCOUNTABILITY

El término “accountability” tiene distintas traducciones dependiendo del contexto. Respecto a la protección de datos personales, se ha tomado como el principio de Responsabilidad proactiva o demostrada entendido como el basado en el enfoque del reconocimiento y compromiso de las organizaciones, a los efectos de adoptar los estándares de protección que aseguren a los ciudadanos un tratamiento adecuado de sus datos personales.

En cuanto a la seguridad de la información, accountability se utiliza también como trazabilidad, que hace referencia a la inclusión de controles que permitan realizar un seguimiento completo de una determinada acción, al registrar usuarios, fechas, operaciones, etc. Cuando se hace referencia a las actividades de las personas, se utiliza como quien efectivamente hace las actividades, se usa como “rendición de cuentas”.

PROTECCIÓN A LA DUPLICACIÓN

La “protección a la duplicación” es una propiedad que tiene como objetivo asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario, como podría ser requerido en una receta médica o en un papel-billete en el mundo físico.

NO REPUDIO

La propiedad de “No repudio” es necesaria cuando se requiere evitar que una entidad que haya enviado o recibido información, o realizado una transacción, alegue ante terceros que no lo ha hecho. De esta manera, los controles que propicien el no repudio tienden a asegurar que una fuente u origen de un mensaje pueda ser creíble. En el ámbito comercial, por ejemplo, asegurar esta propiedad puede asociarse a los controles para asegurar la confianza en el origen.

CONFIABILIDAD

La “confiabilidad” tiene como objetivo que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones. Es evidente que para incorporar controles que den cumplimiento a esta propiedad, es necesario contar con información del nivel adecuado a la toma de esas decisiones, así como de la misión de una organización e interiorizarse de sus funciones.

La disciplina seguridad de la información contempla un conjunto de prácticas que han resultado efectivas tanto para especialistas como para instituciones. En particular, existen estándares de distintas entidades con conocimientos y experiencia que identifican y describen estas prácticas y las compilan en distintos tipos de normas, siguiendo además un programa de revisión de los documentos y de los temas que requieren nuevas definiciones.

Los marcos internacionales de referencia en Seguridad de la información

Para asegurar el cumplimiento de las propiedades de la seguridad de la información existen marcos de referencia conformados por buenas prácticas elaboradas por entidades especializadas en materia de tecnología y estándares.

En este sentido, cuando las regulaciones o legislación abordan los riesgos de seguridad de la información, suelen utilizarse como referencia uno de los siguientes marcos internacionales, o alguna adaptación, porque están elaborados desde organizaciones internacionales especialistas en la materia.

A continuación, se listan una serie de marcos de referencia internacionales reconocidos:

- La familia de normas ISO/IEC 27000 está conformada por más de 50 documentos, entre los que destacan la ISO/IEC 27001 e ISO/IEC 27002. El primero detalla los requerimientos para un Sistema de Gestión de Seguridad de la Información (SGSI) y el segundo refiere a Controles de Seguridad y Privacidad de la información que aplican a un SGSI.
- La serie de publicaciones especiales del Instituto Nacional de Estándares y Tecnología (NIST) de la Oficina de Comercio de Estados Unidos, integrado por más de 150 documentos en su línea SP-800 dedicada a la seguridad y privacidad, y su marco de referencia en temas de ciberseguridad (Cyberframework), y en particular el SP 800-53 rev. 5 “Controles de seguridad y privacidad para sistemas de información y organizaciones”.
- Los Controles CIS del Centro para la Seguridad de Internet, organización no gubernamental de participación público-privada.
- El modelo de ciberhigiene del SEI, el Instituto de Ingeniería de Software de la Universidad de Carnegie Mellon para pequeñas organizaciones, que es un subconjunto de prácticas extraídas del Modelo de Madurez de Resiliencia (RMM) utilizado para grandes organizaciones e infraestructuras críticas.

Para el ámbito de la Administración Pública Nacional de Argentina, la Decisión Administrativa Nro 641/2021 funciona como un conjunto de buenas prácticas, o prácticas efectivas, elaboradas especialmente con requerimientos para ese ámbito que tienen su referencia principal en el estándar ISO/IEC 27001:2013.

Otro ejemplo puede ser el caso de la República Oriental del Uruguay, donde se adoptó el Marco de Referencia en ciberseguridad del NIST como modelo para la ciberseguridad a nivel Nacional.

Cada uno brinda una guía para la implementación de controles dirigidos al cumplimiento de los objetivos de seguridad de la información.

En el caso de los marcos de referencia internacionales, es necesario destacar que se conforman como una serie de documentos dado que la implementación de seguridad de un sistema de gestión requiere de una cantidad de información adicional para poder implementarse, como metodologías y lineamientos sobre el riesgo, guías técnicas, lineamientos para las actividades de gobernanza, etc.

Adicionalmente, entre otras instituciones que emiten documentos sobre ciberseguridad y las disciplinas relacionadas, puede mencionarse a:

ENISA, hoy Agencia europea de ciberseguridad, su nombre original en inglés era European Network and Information Security Agency; (ISP)2, Consorcio Internacional de certificación de Seguridad de sistemas, e ISACA; estas últimas dos organizaciones no gubernamentales internacionales son las principales emisoras de certificaciones en distintas disciplinas de ciberseguridad.

Los temas o áreas de seguridad de la información para una organización de acuerdo a los estándares internacionales pueden agruparse en las siguientes categorías:

1. Aspectos relacionados con el gobierno o gobernanza de la ciberseguridad
2. Aspectos de gestión de la seguridad de la información
3. Gestión de activos (procesos, software, hardware, redes)
4. Protección en la gestión de datos
5. Gestión de identidades y controles de acceso
6. Seguridad aplicada a las personas o RRHH
7. Seguridad del espacio físico y del ambiente
8. Seguridad de las redes
9. Seguridad de los sistemas y aplicaciones
10. Seguridad en el desarrollo y sus componentes
11. Gestión de amenazas y vulnerabilidades
12. Gestión de incidentes de seguridad de la información
13. Aspectos de la continuidad y resiliencia
14. Seguridad en las relaciones con terceras partes
15. Requisitos de cumplimientos, contractuales, regulatorios y legales
16. Aseguramiento de los procesos.

Un modelo de gestión se refiere al conjunto de actividades que se requieren para la planificación, implementación, operación, seguimiento y control de las actividades requeridas para dar cumplimiento a los objetivos fijados. En particular, por ejemplo, la norma ISO/IEC 27001 contiene lineamientos para un sistema de gestión de seguridad de la información y la ISO 22301 trata sobre el desarrollo e implementación de un Sistema de gestión de Continuidad del negocio.

En una organización pequeña o mediana es esperable que los distintos procesos se ensamblen de manera coordinada a medida que se crece en tamaño y complejidad.

¿Por qué son necesarios los modelos de madurez en materia de seguridad de la información?

Como se mencionó anteriormente, algunos marcos internacionales despliegan un conjunto de documentos para incorporar un marco de gestión de la seguridad de la información y prácticas efectivas estandarizadas. A lo largo de estos últimos años fueron adaptando su contenido para incluir actividades novedosas así como nuevos enfoques.

En este sentido, los modelos de madurez se elaboran para la implementación y evaluación de metas concretas y para poder realizar planes de acción con plazos, en función de los recursos y los objetivos a alcanzar.

Por ejemplo, en el Modelo de controles CIS existen 3 Grupos de implementación, dependiendo de las características de la organización y de las capacidades técnicas con las que cuente.

La implementación de un conjunto completo de buenas prácticas, que incluyan una metodología de gestión de riesgos puede ser un proyecto desalentador para empresas pequeñas; para esos casos, existen modelos de madurez que plantean etapas o niveles, con métricas para avanzar en base a un camino o etapas de mejoras preestablecidas.

En otros casos, los conjuntos de controles se agrupan por niveles de acuerdo a los recursos disponibles, al tipo de industria, los tipos de datos de clientes y clientas y capacidades de las personas que pertenecen a la organización.

¿En qué consisten la continuidad de los servicios, la resiliencia y la ciberresiliencia?

Gestión de la Continuidad del Servicio

El proceso de gestión de continuidad de los servicios para un organismo público, o continuidad del negocio como se denomina en el contexto empresarial, es crítico. Su objetivo es la planificación y preparación ante eventos que puedan interrumpir la provisión de servicios o la entrega de productos, es decir la implementación de un entorno en el que se minimicen los impactos más graves para la organización y permita una recuperación acorde con la criticidad del servicio o proceso afectado.

Este proceso incorpora aspectos que exceden el alcance de la tecnología y seguridad de la información, porque la esfera de decisión sobre la misión de la organización o del negocio corresponde a sus máximas autoridades.

Son ejemplos de eventos de interrupción que deberían analizarse, un corte eléctrico de magnitud, un incendio, un terremoto o maremoto, una manifestación que impida el acceso del personal, una inundación, etc.; eventos que se presumen de baja probabilidad de ocurrencia pero de un impacto alto.

Otro aspecto que por la descripción hecha hasta el momento resulta importante resaltar es que en la “Continuidad del negocio”, el aspecto de seguridad física, medioambiental y edilicia está presente.

El concepto de resiliencia y de ciberresiliencia

El concepto de resiliencia incorpora en el análisis de la seguridad de los procesos la planificación de las actividades necesarias para poder recuperarse ante incidentes graves o gravísimos de cualquier tipo.

A esta capacidad se denomina resiliencia. La preparación para recuperarse y continuar operando a un nivel aceptable ante cualquier tipo de incidente de seguridad de la información se denomina ciberresiliencia.

Un ejemplo de ciberresiliencia podría ser cuando una organización mantiene su información confidencial cifrada y con los respaldos apropiados. En ese caso, al verse afectada por un incidente de ransomware, podrá seguir operando y la información comprometida, aunque filtrada, seguirá preservando la confidencialidad.

¿A qué se llama ciberseguridad?

En las últimas décadas, los impactos de los incidentes de seguridad de la información se han expandido desde las organizaciones a las sociedades y a los países. Éstos impactos a nivel país tienen mayor alcance, en tanto se abordan aspectos de la seguridad en los servicios esenciales y sus infraestructuras críticas, el comercio internacional o las atribuciones de los ataques que se originan en un país y afectan a civiles de otros países o a sus infraestructuras, los espionajes industriales y entre países. Estas nuevas ramificaciones merecen análisis multidisciplinar. Además, las consecuencias afectan desde derechos fundamentales como la libertad de expresión, la privacidad, la protección de datos personales hasta la defensa nacional.

En el contexto de los problemas que afectan a la ciudadanía se adopta el uso del término "ciberseguridad", no existiendo aún una definición con consenso internacional.

Adicionalmente, para el público en general, varios términos se usan de manera indistinta. Se debe tener en cuenta que para diferentes ámbitos puede tener definiciones distintas. En este sentido, las normas ISO han adoptado para ciberseguridad una definición en la ISO/IEC 27100 en el año 2020 comentada a continuación:

Ciberseguridad: Resguardo* de las personas, la sociedad, las organizaciones y las naciones de los ciberriesgos**, entendiendo por ciberriesgo como el efecto de la incertidumbre sobre los objetivos establecidos.

→ Adicionalmente en la definición se incluyen las siguientes tres aclaraciones:

- 1ero. Cuando se refiere a *Resguardo significa mantener el ciberriesgo en un nivel tolerable.
- 2do. ** El ciberriesgo puede expresarse como efecto de la incertidumbre de una entidad en el ciberespacio.
- 3ero. El ciberriesgo está asociado con la posibilidad de que las amenazas exploten las vulnerabilidades en el ciberespacio y, por lo tanto, causen daño a las entidades.

Por otro lado, define Ciberespacio como el entorno digital interconectado de redes, servicios, sistemas, personas, procesos, organizaciones y lo que reside en el entorno digital o lo atraviesa.

Es importante que la terminología sea clara y coherente desde los aspectos organizacionales y a nivel país, dado que en general la regulación suele basarse en éstas definiciones, y ante disputas legales, las interpretaciones pueden ser críticas.

Una consideración relevante de la definición de ciberseguridad de ISO/IEC 27100 y en algunas otras que suelen utilizarse, es que parecen excluir el entorno físico asociado al entorno digital, mientras que se encuentran presentes en las buenas prácticas de seguridad de la información así como es evidente en la práctica profesional la importancia de proteger el

espacio físico asociado, que alcanza a la provisión de los servicios básicos, el cableados, y la información en otros soportes asociado a los servicios digitales.

Cabe mencionar que Argentina cuenta con la Resolución Nro. 1523/2019 en la que se ha adoptado un glosario de ciberseguridad que, de acuerdo a su texto, se actualizará de acuerdo a la evolución tecnológica.

En el contexto de las organizaciones, no ya a nivel de Estados, el término de ciberseguridad se utiliza también para englobar a la seguridad informáticas, la seguridad de la información, también aspectos legales relacionados y la gestión de los riesgos de tecnologías como una categoría, aunque muchas veces, como se ha mencionado, se la nombre como sinónimo de seguridad informática.

Volviendo al ámbito nacional, la ciberseguridad está presente en las relaciones internacionales, por un lado cuando se interviene para promover la protección de servicios e infraestructuras civiles de ataques originados en el extranjero (por individuos o grupos) como para la protección de personas, infraestructuras y organizaciones de ataques de Estados extranjeros.

En ambos contextos se puede apreciar que la protección del entorno físico es inherente a la protección de servicios digitales y de la información, la seguridad de la infraestructura que les da soporte, así como la de los elementos físicos que interactúan o almacenan algún tipo de información necesaria (discos rígidos externos, dispositivos USB, código QR en papel, etc.) para el funcionamiento de algún servicio digital. De esta manera, la protección del entorno físico asociado al ámbito que procesa información como pueden ser los puertos de conexión de un dispositivo, el cableado por el que circulan los datos, o su soporte de almacenamiento son también parte del ambiente en la ciberseguridad.

Ciberseguridad y Ciberdefensa

Para identificar un panorama general podemos decir que en nuestro país el ámbito de la defensa nacional es el de la protección de la integridad territorial, la soberanía y la independencia. En ese sentido la infraestructura edilicia y tecnológica que constituye el sistema de defensa también está dentro de su alcance.

Las herramientas de la ciberseguridad, sus prácticas y herramientas en este caso, se ponen a disposición del objetivo de la defensa nacional, para asistir en cada una de las actividades y también en lo que son sus acciones en escenarios de conflictos.
Consideran al ciberespacio, de acuerdo a la última Política de ciberdefensa, como el conformado por la “infraestructura tecnológica, de propiedades físicas y virtuales, desplegada territorialmente, que permite la creación, procesamiento, almacenamiento, transporte y destrucción de información mediante el empleo de las tecnologías de la información, la operación y la comunicación”.

En este sentido, identifica que el ciberespacio constituye una nueva dimensión con características particulares pero que no es independiente de los espacios tradicionales (tierra, mar, aire y espacio) sino que se trata de una dimensión que los atraviesa a todos.

Competencias en ciberseguridad

En función de seguir las definiciones previas diremos que las competencias en ciberseguridad son las necesarias para abordar las distintas disciplinas abarcadas.

Las funciones y las prácticas de cualquiera de los modelos de gestión que aborde aspectos de la seguridad de la información y ciberseguridad requieren conocimientos y habilidades especializadas en distintos campos, desde los aspectos más técnicos, a los temas de gestión de riesgos, así como aspectos legales de varias ramas del derecho. Por este motivo es necesario contar con personal calificado o bien promover la formación en las distintas especialidades, desde los aspectos relacionados con las tecnologías, hasta los más funcionales y de gobierno. Se sugiere contar con un diseño de perfiles que puedan acompañar las necesidades del modelo de gestión que su organización adopte.

Cabe mencionar que la seguridad de la información es un proceso y no un producto. Por más que se invierta en tecnología, si no se incorporan las prácticas en la cultura de la organización, el programa de ciberseguridad no estará completo.

Tener un panorama general de las competencias necesarias para las actividades de gobierno, gestión y operación es primordial tanto para prevención, contención y respuesta para todas las áreas de la ciberseguridad como en la ciberdefensa.

En este sentido es importante que haya formación de especialistas en las distintas ramas de aplicación como en las distintas especialidades de la seguridad informática.

Mecanismos de aseguramiento. El modelo de las tres líneas y la auditoría

El modelo de 3 líneas, antes llamado “3 líneas de defensa” se refiere a los diferentes niveles de responsabilidad en la gestión de riesgos en una organización. La primera línea la forman empleadas, empleados y las y los de la organización, que son responsables directos de la gestión de los riesgos operativos y la implementación de los controles internos.

La segunda línea se refiere a las funciones de gestión de riesgos y del control interno, que se encargan de monitorear y supervisar los controles internos implementados por la primera línea de defensa. Estas funciones de la segunda línea pueden incluir las áreas de gestión de riesgos, cumplimiento, ciberseguridad o calidad. La tercera línea se refiere a la función de auditoría interna, que evalúa la eficacia de los controles internos y la gestión de riesgos en toda la organización. La auditoría interna también brinda asesoramiento y recomendaciones para mejorar la eficacia de los controles internos y la gestión de riesgos en la organización.

Desde el punto de vista del área auditada, debe tenerse presente que el cumplimiento de los requisitos requiere de un respaldo, que a los efectos de la auditoría corresponden a la evidencia que será relevada durante las acciones de auditoría.

En este sentido, cada marco de referencia o normativa cuenta con una serie de controles y objetivos cuyo desempeño es importante documentar para probar el cumplimiento oportunamente ante la auditoría. Adicionalmente, también es relevante señalar que los controles se implementan para minimizar riesgos y con esa finalidad presente se debe realizar la documentación.

Debe recordarse que ante obstáculos o impedimentos para cumplir con un requisito en particular, pueden implementarse controles compensatorios que mitiguen ese riesgo, documentando tanto los obstáculos como los nuevos controles.

La ciberseguridad y la ciberdelincuencia

En la medida que los servicios digitales se extienden y alcanzan a los aspectos más importantes de nuestra vida también nos vuelven más dependientes de las tecnologías de la información. En este sentido, existen sistemas de información y aplicaciones desde hace varias décadas y todos los días se suman nuevos. Aumentan las interconexiones e interdependencias, y es así que los sistemas y aplicaciones se vuelven también más complejos.

Desde ya hace tiempo, un sinnúmero de debilidades de sistemas operativos, sistemas de información y aplicaciones son aprovechadas por quienes delinquen para causar daños de todo tipo, llegando a conformar uno de los rubros del crimen organizado que más dinero involucra. Estas vulnerabilidades también son explotadas, en menor grado, en campañas de activismo y por agencias de inteligencia.

La ciberseguridad pasa a tener relevancia, ya no como de interés interno de cada organización pública o privada, sino como un valor social y económico, ya que la falta de adecuación a las buenas prácticas en la materia, mientras no haya regulación, será esencial para la protección de la información y los servicios de todo tipo.

Las personas que delinquen se han aprovechado de vulnerabilidades técnicas, en procedimientos organizacionales, así como se han vuelto hábiles para engañar a las personas y “robar” información confidencial de organizaciones de cualquier tipo. Acceden a información y luego la ofrecen a la venta, extorsionan con publicar información secreta y llegan a impedir el funcionamiento de empresas hasta lograr la quiebra, en varios casos documentados.

Otro aspecto es el relacionado con la protección de la confidencialidad de la información que tiene implicaciones enormes, en tanto puede afectar la privacidad de las personas en sus aspectos más íntimos pero también son problemas para las empresas en sus secretos industriales, y hasta puede afectar secretos de Estado, si no se toman medidas técnicas, organizativas y estructurales que abarquen al conjunto de la sociedad.

La ciberseguridad, en tanto medidas para la protección y defensa, así como en la respuesta ante incidentes, es la fuente principal de fortalecimiento para hacer frente al avance de la delincuencia que se aprovecha de este tipo de debilidades.

Referencias

Buenas prácticas en seguridad de la información y ciberseguridad

Publicaciones NIST.
https://csrc.nist.gov/Publications

NIST- Serie 800 de seguridad de la información
https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

Publicaciones ISO/IEC
https://www.iso.org/standard/73906.html

ISO/IEC 27000
https://www.iso.org/standard/73906.html

ISO/IEC 27001
https://www.iso.org/standard/27001

ISO/IEC 27100
https://www.iso.org/standard/72434.html

Controles CIS del Centro para la Seguridad de Internet
https://www.cisecurity.org/controls/v8_pre

Ciberhigiene de la Universidad de Carnegie Mellon
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508765

Modelo de Madurez en Resiliencia de la Universidad de Carnegie Mellon - 2016
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084

Normativa de la República Argentina

Normativa de Seguridad de la Información y ciberseguridad. Decisión Administrativa Nro 641/2021 - Requisitos Mínimos de Seguridad de la Información para la Administración Pública Nacional.
https://www.argentina.gob.ar/normativa/nacional/decisi%C3%B3n_administrativa-641-2021-351345/texto

Resolución Nro 1523/2019
https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918

Normativa en Protección de datos personales. Ley 25326.
http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

Resolución 47/2018
https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-47-2018-312662

Organizaciones que emiten buenas prácticas y contenidos de ciberseguridad. ENISA Agencia Europea de Ciberseguridad
https://www.enisa.europa.eu/

(ISC)2
https://www.isc2.org/

ISACA
https://www.isaca.org/

Organizaciones que emiten buenas prácticas y contenidos de Tecnología y ciberseguridad

NIST - Instituto Nacional de Estándares y Tecnología de Estados Unidos.
https://www.nist.gov/

ISACA
https://www.isaca.org/

República Oriental del Uruguay. Adopción del Marco de Ciberseguridad de NIST
https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad

Seguridad de la información y ciberseguridad

FUNDACIONSADOSKY.ORG.AR

Fundación SADOSKY
Ministerio de Ciencia, Tecnología e Innovación Argentina