ADEN

FUNDAMENTOS DE CIBERSEGURIDAD

AUTOR: JORGE MARIO OCHOA VÁSQUEZ

CONTENIDO

INTRODUCCIÓN

Según el diccionario de la Real Academia Española, el adjetivo 'seguro' significa que está "libre y exento de peligro o riesgo", también puede significar que "no falla o que ofrece confianza". En el entorno digital, la ciberseguridad se refiere a la protección de la información desde el punto de vista de confiabilidad, disponibilidad e integridad de los datos.

El tema de la seguridad de la información en esta era digital es sumamente importante. La ciberseguridad se encarga de proteger la información propia, o de terceros, que se maneja en dispositivos electrónicos y redes.

Es por ello que esta semana exploraremos la importancia de la ciberseguridad, las políticas y elementos de la Seguridad de la información y los factores que conciernen al riego dentro de las organizaciones.

01

¿POR QUÉ ES IMPORTANTE LA CIBERSEGURIDAD?

Mantener nuestro número de identificación, cuenta de banco, direcciones y hasta los patrones de consumo de manera confidencial, es necesario. Para englobar todos los motivos que competen a la ciberseguridad, está el hecho de que la información tiene un valor.

Para ejemplificar la importancia de la ciberseguridad, veamos qué sucedió en 2015 con el sitio web de Ashly Madisson, una red social cuyo slogan era “Life is short. Have an affair”. Dicha página contenía una extensa data de información confidencial y sensible de sus suscriptores.

Impac Team estuvo detrás del ataque, que reveló la data de unos 37 millones de clientes en la dark web -aproximadamente unos 10 gigabytes de datos revelados-. Meses antes, el grupo mandó una advertencia al publicar 40 megabytes de datos, que incluían nombres, direcciones de correo electrónico, números de teléfono móvil e información de tarjetas de crédito. Los cibercriminales amenazaron con revelar la lista completa a menos que el sitio de Ashley Madison y su web asociada, Established Men, fueran sacados de línea permanentemente. La empresa canadiense dueña de ambos sitios, Avid Life Media, se negó y, como consecuencia, la lista fue revelada.

La preocupación de muchos usuarios originó que la compañía ofreciera un borrado completo de su perfil, mensajes y fotos, un servicio que antes tenía un costo. Sin embargo, los cibercriminales alegaron que aquello era una mentira.

Este ataque afectó a más de 50 países y fue investigado por el FBI, la Real Policía Montada de Canadá, la Policía Provincial de Ontario y los Servicios de Policía de Toronto.

Como vemos, la filtración de información sensible tiene un coste monetario, tanto por el robo o por la pérdida de clientes, y puede ocasionar daños irreversibles, como arruinar la reputación de una persona, empresa u organismo. Para evitarlo, debemos tener un Sistema de Gestión de Seguridad de la Información (SGSI).

02

LAS V DE BIG DATA

El término Big Data aparece a comienzos de 1990 para referirse a un conjunto amplio de datos. Sus características y propiedades específicas permiten comprender las ventajas y desafíos de la estrategia de datos de una compañía. Así, tenemos las diez V de Big Data:

1. **Volumen:** indica cuánta data se genera por unidad de tiempo. Por ejemplo, Youtube almacena 18.000 segundos de video por minuto de sus usuarios, esto equivale a unas 300 horas de video subidas por minuto a la plataforma.

2. **Velocidad:** hace referencia a la velocidad con que se generan, producen, crean o actualizan los datos. El motor de búsqueda de Google procesa unos 3,5 mil millones de búsquedas por día, equivalente a 40.000 búsquedas por segundo.

3. **Variedad:** los datos que maneja principalmente son no estructurados, sin embargo, también se manejan datos estructurados y semiestructurados.

4. **Variabilidad:** se refiere tanto en el número de inconsistencias de los datos, como a la multitud de dimensiones de datos. También puede indicar la velocidad inconsistente a la que se cargan grandes datos en bases de datos.

5. **Veracidad:** es relativo a la confianza ¿Podemos confiar en la data? Es directamente proporcional a la fiabilidad del análisis basado en ella. Por ejemplo, si se tiene la data de los últimos 5 años de los clientes de varias tiendas y los precios, usted puede formular las siguientes preguntas: ¿quién creó la fuente?, ¿qué metodología se usó para recopilar los datos?, ¿solo se incluyeron ciertos tipos de tiendas de ropa, accesorios, tiendas departamentales?, ¿los creadores de datos resumieron la información?, ¿la Data ha sido editada o modificada por alguien más?

6. **Validez:** define si la data es precisa y correcta. Va de la mano con la veracidad y requiere de buenas prácticas de gobernanza de datos para garantizar la calidad del análisis. Aproximadamente el 60% del tiempo de un científico de datos se consume en limpiar sus datos antes de cualquier análisis.

7. **Vulnerabilidad:** qué tan susceptible es la data de sufrir una filtración. Esto es un problema actual y que tiene consecuencias graves, tal como vimos en la sección anterior con el caso de Ashley Madison.

8. **Volatibilidad:** referente a cuánto tiempo debe estar disponible la data según su vigencia. Anteriormente, esta se almacenaba indefinidamente, pero hoy en día, con la velocidad, volumen y el costo que ello implica, surge la necesidad de diseñar reglas acordes a las necesidades de la empresa.

9. **Visualización: a**ctualmente, hay desafíos técnicos debido a las limitaciones de la tecnología en memoria y a la escasa escalabilidad, funcionalidad y tiempo de respuesta. El uso de gráficos tradicionales no es confiable por el volumen, la variedad y la velocidad de los macrodatos, además de sus relaciones complejas. Por lo que se necesitan diferentes formas de representar datos, por ejemplo, haciendo uso de la agrupación de datos, mapas, coordenadas, diagramas entre otros.

10. **Valor:** representa el término comercial de la data, el motivo de su análisis. Quizás usted quiere comprender mejor a sus clientes, optimizar los procesos y mejorar el rendimiento de la máquina o del negocio.

2.1. ELEMENTOS DE LA SEGURIDAD DE LA INFORMACIÓN

La transformación digital, junto con el aumento del uso de servicios de almacenamiento, trae consigo muchas ventajas y, a su vez, se asocia con mayores riesgos cibernéticos. Por consiguiente, es imperante contar con un Sistema de gestión de seguridad de la información (SGSI).

Se entiende que la Seguridad de la información es un proceso integrado, que protege la identificación y gestiona la información y los riesgos a los que esta es susceptible. En este orden de ideas, la Seguridad de la información abarca todas las medidas tanto de prevención como de reacción del individuo y/o la organización, así como las tecnologías para proteger dicha información, manteniendo la confidencialidad, la autenticidad y la integridad.

En este sentido, hay tres elementos clave en el proceso: las personas, los procesos y la tecnología.

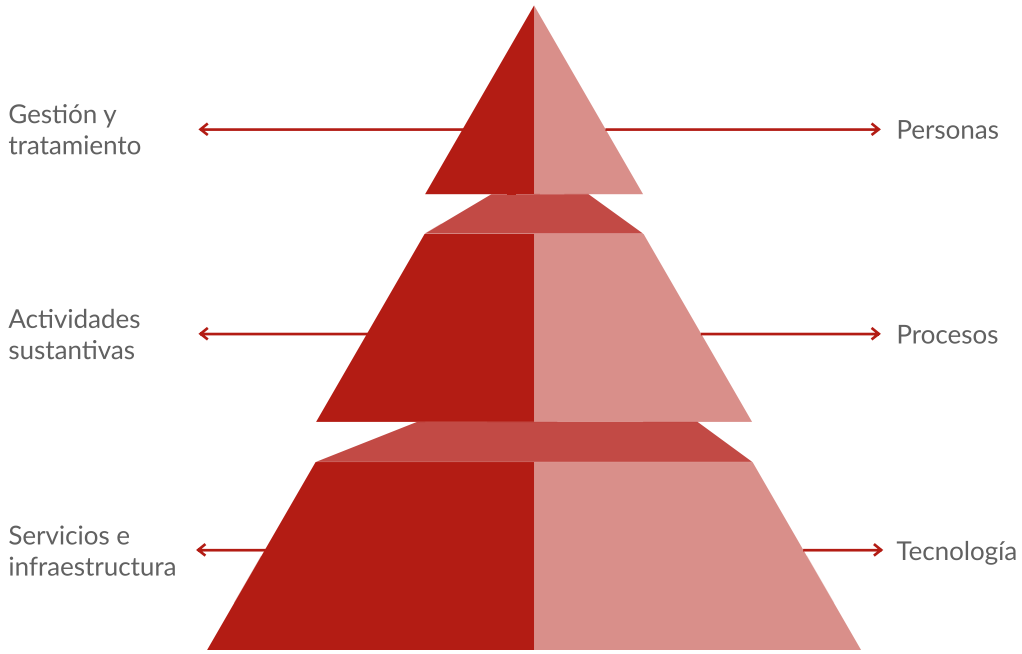


Figura 1. Elementos de la Seguridad de la información (Elaboración propia, 2021)

Personas: encargadas de la gestión y el tratamiento de la información. Pueden ser empleados, directivos, autoridades competentes, clientes, proveedores, contratistas y/o prestadores de servicio.

Procesos: abarca todas las actividades que se realizan para cumplir con los objetivos planteados. Es la parte vulnerable por incluir o depender de la información.

Tecnología: está ligada a los servicios e infraestructura de la empresa por ser la que lleva el manejo y desarrollo de la información. Además, se encarga de almacenar, recuperar, difundir y darle mantenimiento a los datos de valor que se encuentran ahí.

03

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La norma ISO 27001 es una norma internacional creada por la Organización Internacional de Normalización (ISO) para garantizar buenas prácticas de seguridad de la información. En términos simples, la norma asegura, integra y mantiene de forma confidencial toda la información de la compañía y los sistemas que la almacenan. Paralelamente, la implementación de esta norma permite evaluar y controlar los riesgos que se hayan identificado mediante la creación de un plan que ayude a prevenirlos y, en caso de presentarlos, tener una guía para mitigar su impacto. Debe señalarse que la norma ISO 27001 cuenta con una certificación que permite generar confianza a sus empleados, proveedores y clientes de manera que mejora la reputación de su empresa.

Esta norma puede aplicarse a cualquier tipo de empresa, sin importar su industria o tamaño. En efecto, la norma ISO 27001 contiene la metodología que la empresa debe seguir para implementar el SGSI exigido por muchos países y, al mismo tiempo, permite que la empresa:

- Obtenga un diagnóstico por medio de entrevistas.
- Realice un análisis exhaustivo de todos los riesgos que se puedan presentar.
- Cree un plan de acción acorde a las necesidades de la empresa.
- Diseñe manuales y procedimientos.

- Monitoree y revise el desempeño y la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI).

- Adopte prácticas que favorezcan el mejoramiento continuo con base en la medición del objetivo.

3.1. ESTRUCTURA DE LA NORMA ISO 27001

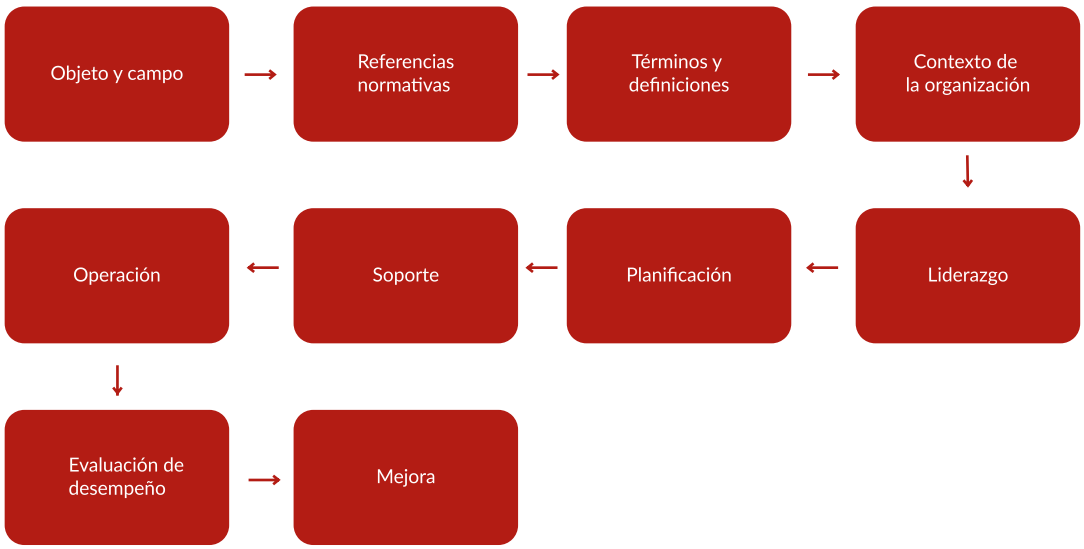


Figura 2: Estructura de la norma ISO 27001 (Elaboración propia, 2021)

En referencia a la figura 2, se describe cada etapa del proceso:

- **Objeto y campo de la aplicación:** comprende las herramientas para saber el uso, aplicación y beneficio de la norma.

- **Referencias normativas:** engloba todos los documentos que se deben tener en cuenta para aplicar las recomendaciones de la norma.

- **Términos y definiciones:** es un glosario con las palabras clave.

- **Contexto de la organización:** busca entender el contexto de la empresa y cuáles son sus necesidades, para verificar cuál será el alcance del Sistema de Gestión de Seguridad de la Información que se va a aplicar.

- **Liderazgo:** los líderes de la empresa nombran a los responsables y publican, oportunamente, las políticas establecidas. En este sentido, todos los empleados deben estar enterados sobre los planes de acción que se van a llevar a cabo y de qué manera ellos contribuyen a su cumplimiento.

- **Planificación:** se establecen los objetivos y el camino a seguir para lograrlos.

- **Soporte:** son los recursos necesarios que les permitan ser competentes, contar con una óptima comunicación y documentar la información requerida para cada caso.

- **Operación:** implica planificar, implementar, monitorear y controlar cada uno de los procesos, valorar cada riesgo y crear una solución para cada uno de ellos.

- **Evaluación de desempeño:** se realiza el seguimiento, la medición, el análisis y la evaluación del sistema implementado, con el fin de verificar que se esté cumpliendo con lo establecido.

- **Mejora:** se trata de identificar qué aspectos no están funcionando correctamente para poder ajustarlos y cumplir con su objetivo final.

3.2. PROTOCOLOS DE LA SEGURIDAD DE LA INFORMACIÓN

En cada búsqueda en internet se genera, inconscientemente, un intercambio de datos con las páginas que se visita. A continuación, los protocolos que previenen

- **Cifrado de datos:** oculta la información enviada, hasta que esta llegue al receptor.

- **Lógica:** mantiene la coherencia con el orden de los datos del mensaje, el significado y el momento en que se va a enviar.

- **Autenticación:** garantiza que la información está siendo manipulada por un ente autorizado y no está sufriendo algún tipo de intervención por agentes externos.

El SGSI debe estar enfocado en cuatro fundamentos:

Disponibilidad	Confidencialidad	Integridad	Autenticación
Disponer de la información necesaria y al momento, procurando que el Sistema no tenga problemas o que algún ente externo acceda de manera ilícita.	Es la información que solo está disponible para el personal autorizado y no debe ser distribuida por terceros.	La información registrada debe ser correcta y no tener errores o modificaciones. Esto evita amenazas externas y errores humanos.	Esta información la suministra directamente un usuario y se debe validar que los datos otorgados sean los correctos.

Un SGSI define los procedimientos y controles para cumplir con la legalidad y la protección de los datos, además de establecer las políticas que deben conocer todos los miembros de la organización e identifica los riesgos y ataques que pueden sufrir y de qué manera se pueden mitigar, teniendo en cuenta que el riesgo siempre está presente.

Un SGSI, según la norma ISO 27001, debe incluir los siguientes elementos:

1.Manual de seguridad

Es la guía de cómo se debe implementar y seguir el SGSI. Este documento contiene toda la información: objetivos, alcance, responsables, políticas, directrices, entre otras actividades que se decidan llevar a cabo.

2.Procedimientos

Este documento comprende las actividades operativas y proporciona los parámetros que se deben seguir para que la gestión sea eficaz y la planificación, operación y control sean los adecuados.

3.Instrucciones

Es la descripción paso a paso de cuáles son las tareas y actividades que se deben cumplir para que la gestión sea eficiente.

4.Registros

Es la evidencia de la información que ha sido documentada durante toda la gestión, con ella se verifica que se esté cumpliendo con los objetivos propuestos.

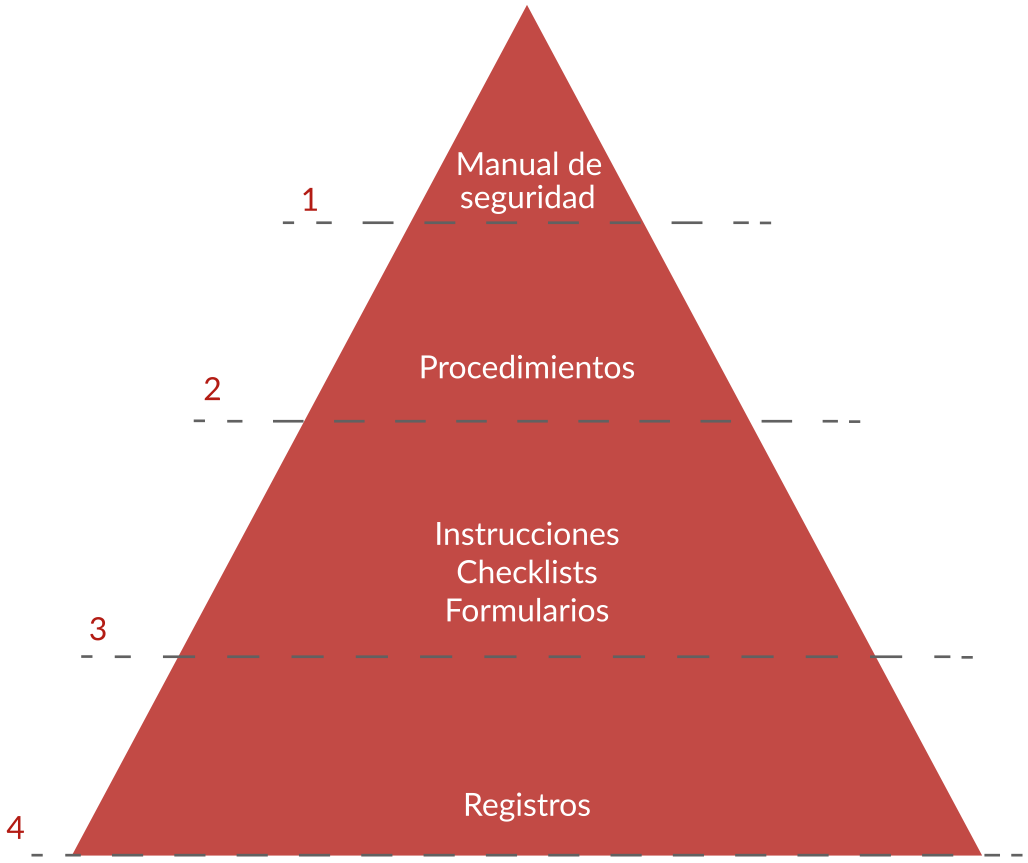


Figura 3. Partes de un SGSI según la norma ISO 27001 (Elaboración propia, 2021)

Conocidas las partes de un SGSI, se deben seguir los siguientes pasos para implementarlo:

1.Definir la política de seguridad

Abarca la determinación de los objetivos, el marco general, los requerimientos legales y los criterios con los que serán evaluados los riesgos, con base en la metodología aprobada por la Dirección o la Junta directiva.

2.Definir el alcance del SGSI

Establece los límites y estima los logros del plan de acción en la organización, teniendo en cuenta los activos, las tecnologías y la descripción de cada uno.

3.Identificar los riesgos

Se reconocen las posibles amenazas a las que puede estar expuesta la compañía y se identifican quiénes son los responsables directos, a qué son vulnerables y cuál sería el impacto en caso de que se llegue a violar la confidencialidad, la integridad y la disponibilidad de los activos de información.

4.Analizar y evaluar los riesgos

Se evalúa el impacto que tendría alguno de los riesgos si se llegara a materializar. Además, se identifica cuál es la probabilidad de ocurrencia y cómo esto podría afectar a los controles que ya están implementados. De igual manera, se debe verificar si se puede aceptar el riesgo o debe ser mitigado.

5.Hacer un tratamiento de riesgos

Consiste en implementar los controles adecuados, clasificar los niveles de riesgo, evitarlos o transferirlos a terceros si es posible.

6.Declarar la aplicabilidad

Se establecen los objetivos de control y se escogen los controles que se van a implementar.

7.Realizar la gestión

Se aplica el tratamiento de riesgos teniendo en cuenta los controles que fueron identificados en las etapas anteriores. Asimismo, se define el sistema de métricas.

Junto con la gestión de operación y los recursos necesarios para su cumplimiento, también se genera conciencia dentro de la organización y se fomenta una cultura que permita que todos los empleados conozcan el SGSI.

8.Monitorear

Periódicamente, se debe hacer una revisión del SGSI para identificar si está cumpliendo -y si es efectivo- lo que señala la norma ISO 27001. Es necesario reportar las mejoras que deben hacerse y cuáles serán las acciones a ejecutar para lograr esto.

3.2.1.Ventajas de implementar un SGSI bajo la norma ISO 27001:

- Permite equilibrar y coordinar su proceso de seguridad.
- Permite crear metodologías que ayuden a mitigar el riesgo y aumentar la seguridad de la información disponible.
- En caso de que se llegue a presentar un riesgo, este no resulta en una pérdida tan significativa, gracias al plan de acción eficaz.
- Permite cumplir con los requerimientos legales exigidos por los entes de control.
- La certificación ISO27001 agrega valor a la empresa.
- El uso eficiente reduce los costos.
- Genera confianza con todos los miembros de su organización, ya sean clientes, proveedores o empleados.
- Proporciona la capacidad de activar alertas cuando se produce una actividad sospechosa.
- Permite supervisar los controles de seguridad.
- Es una herramienta que brinda la capacidad de planificar y realizar un seguimiento de los procesos.
- Contribuye a la imagen de la empresa (reputación).
- Proporciona una metodología clara y eficaz.
- Reduce el riesgo de pérdida o robo de información.

3.3. DESARROLLO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El desarrollo de una política de seguridad de la información responde al contexto en el que opera una organización, evaluando las necesidades de control en función de los fines, objetivos, estrategias, estructura y procesos establecidos por la organización.

Una estructura típica documentada en una política de este nivel:

- **Resumen:** política Resumen - Visión general.

- **Introducción:** explicación breve del asunto principal de la política.

- **Ámbito de aplicación:** descripción de los departamentos, áreas o actividades de una organización a las que afecta y/o aplica la política.

- **Objetivos:** descripción de la intención de la política.

- **Principios:** descripción de las reglas que conciernen a las acciones y/o decisiones para alcanzar los objetivos. En algunos casos, es útil identificar previamente los procesos clave asociados con el asunto principal de la política, para pasar posteriormente a identificar las reglas de operación de los procesos.

- **Responsabilidades:** descripción de quién es el responsable de cada acción para el buen funcionamiento de la política. En algunos casos, puede incluir una descripción de los mecanismos organizativos y de las responsabilidades de las personas con roles designados.

- **Resultados clave:** descripción de los resultados relevantes para las actividades de la organización. Se obtienen cuando se cumplen los objetivos.

- **Políticas relacionadas:** descripción de otras políticas relevantes para el cumplimiento de los objetivos, usualmente se indican detalles adicionales en relación a temas específicos.

El objetivo de este control es el de dirigir y dar soporte a la gestión de la seguridad de la información, en concordancia con los requerimientos del negocio, las leyes y las regulaciones.

04

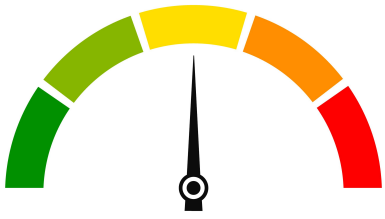
EL RIESGO

Las organizaciones se enfrentan a factores e influencias (externas e internas) que generan dudas sobre si lograrán sus objetivos. En este orden de ideas, se entiende como riesgo al factor de incertidumbre sobre los objetivos. En concordancia, la gestión del riesgo es iterativa y asiste a las organizaciones en establecer su estrategia, lograr sus objetivos y tomar decisiones informadas. Su propósito es la creación y la protección del valor.

4.1. IDENTIFICACIÓN DEL RIESGO

Se deben encontrar, reconocer, clasificar y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos. Para ello es importante contar con información pertinente, apropiada y actualizada.

Se distinguen dos tipos de riesgo: riesgo inherente y riesgo residual.



4.4.1. Riesgo Inherente:

Este tipo de riesgo se encuentra en el ambiente y puede ser originado por factores externos o internos, tal es el caso de:

- Normativas y regulaciones externas.
- Características, políticas y normas de la empresa.
- Estrategias y métodos de trabajo.
- Área financiera.
- Sistemas de control interno.

Las políticas deben ser claras y precisas al indicarle a los usuarios qué pueden hacer y cómo aplicarlo o, en su defecto, indicar a quién dirigirse en caso de duda. Por ejemplo: ¿se pueden hacer fotografías de las instalaciones?, ¿se puede instalar software para uso particular en computadores corporativos?, ¿se puede publicar noticias de la empresa en redes sociales?

Una falta de establecimiento e implantación de políticas permite la materialización de potenciales amenazas, tanto en ciberseguridad como en otros aspectos.

La probabilidad se entiende como la posibilidad de materialización del riesgo analizado. Advierta que es imposible tener una probabilidad cero. Para fines prácticos se utiliza la fórmula:

Riesgo = **Impacto x Probabilidad**

Como su nombre lo indica, es el riesgo específico, asociado a cada trabajo o proceso, por tanto, no se puede eliminar. Lo ideal es mitigar su efecto teniendo en cuenta un plan de acción en caso de que ocurra un imprevisto. Para ello la empresa debe identificarlo e incluirlo en el plan de gestión.

4.4.2. Riesgo Residual:

Es aquel riesgo que subsiste después de haber implementado controles. La acción recomendada es minimizarlo o mitigarlo hasta tener un nivel de riesgo aceptable.

Es importante que la gestión de riesgo atienda primero el riesgo inherente y luego el riesgo residual. Este último refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas.

4.2. EVALUACIÓN Y ANÁLISIS DEL RIESGO

El propósito del análisis del riesgo es comprender la naturaleza y las características del riesgo. Esto implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios y controles.

El análisis del riesgo se puede realizar con diferentes grados de detalle y complejidad, dependiendo del propósito del análisis, la disponibilidad y la confiabilidad de la información y los recursos disponibles.

Este análisis deberá considerar factores, tales como la probabilidad de los eventos y de las consecuencias, la naturaleza y la magnitud de las consecuencias, la complejidad y la interconexión, los factores relacionados con el tiempo y la volatilidad, la eficacia de los controles existentes y los niveles de sensibilidad y de confianza. Las organizaciones pueden utilizar varias técnicas para identificar los riesgos a los que están expuestas. Para la evaluación de riesgo se puede usar la escala Likert de 5 puntos, que mide el grado de importancia del riesgo. Se puede identificar el impacto y probabilidad como:

- **Impacto:** sin impacto, leve, moderado, alto, crítico.

- **Probabilidad**: rara, baja, media, alta, casi seguro.

Con estas variables se elabora una matriz para cada uno de los eventos que se han identificados previamente y, de este modo, que se obtiene el riesgo único para cada evento.

La evaluación de riesgos debe hacerse independientemente de que las fuentes de riesgo estén o no bajo el control de la organización. El análisis del riesgo es necesario para la toma de decisiones sobre la manera de tratar los riesgos -y si es necesario hacerlo-, específicamente con la estrategia y los métodos más apropiados de tratamiento del riesgo.

Las decisiones que ofrece la ISO 31000:2018 no son excluyentes ni ofrecen una respuesta predeterminada infalible, todo depende del análisis correcto en cada caso, considerando el contexto y las consecuencias internas y externas. Algunas decisiones para el tratamiento de riesgos de esta norma son:

- Tolerar el riesgo y no tomar ninguna decisión al respecto.

- Evitar el riesgo, en referencia a no iniciar o continuar con la actividad que genera el riesgo.

- Aceptar o aumentar el riesgo en busca de una oportunidad.

- Proponer acciones para el tratamiento del riesgo.

- Eliminar la fuente de riesgo.

- Modificar la probabilidad o las consecuencias del riesgo.

- Compartir el riesgo mediante contratos, compra de seguros, entre otros.

- Ordenar nuevos análisis, con base en información adicional y/o de mayor calidad.

- Establecer controles o eliminarlos en caso de que el riesgo haya desaparecido.

- Reconsiderar los objetivos.

Para realizar el tratamiento del riesgo se deben tomar en cuenta varias variables: las económicas, las obligaciones de la organización, los compromisos voluntarios y los distintos puntos de vista de los involucrados. Luego, la selección de las opciones para el tratamiento del riesgo deberá realizarse de acuerdo con los objetivos de la organización, los criterios del riesgo y los recursos disponibles.

4.3. TRATAMIENTO DE RIESGOS

Para seleccionar el tratamiento del riesgo se deberán considerar los valores, percepciones e intereses de los involucrados. La organización deberá elegir el medio adecuado para comunicarse con ellos y consultarles sobre estas decisiones. Usualmente algunas partes interesadas pueden aceptar mejor que otras los diferentes tratamientos del riesgo.

La importancia del seguimiento y la revisión de la fase de implementación garantiza que las distintas maneras de tratamiento sean y permanezcan eficaces, aun cuando poseen un minucioso diseño e implementación no siempre se producen los resultados esperados. Cabe destacar que el tratamiento del riesgo puede introducir nuevos riesgos que necesiten gestionarse.

En caso de no contar con opciones disponibles, o bien las opciones disponibles no modifican suficientemente el riesgo, este se debería registrar y mantener en continua revisión. Asimismo, tanto las personas que toman las decisiones, como las partes interesadas, deberán de ser conscientes de la naturaleza y el nivel del riesgo residual después del tratamiento del riesgo.

4.3.1. Gestión de riesgos

- **Políticas para la Seguridad de la información**: se debe establecer un conjunto de políticas para la Seguridad de la información. Estas políticas deben ser aprobada por la Dirección, posteriormente publicadas y comunicadas a los empleados y a todas las partes externas relevantes.

- **Revisión de las políticas para la Seguridad de la información:** las políticas para la Seguridad de la información se deberán planificar y revisar con regularidad, a fin de garantizar su idoneidad, adecuación y efectividad.

4.3.2. Planes de tratamiento del riesgo

El propósito de los planes de tratamiento del riesgo es especificar la manera en la que se implementarán las opciones elegidas, entendiendo las disposiciones que conlleva y el orden en el cual se debe ejecutar.

- La información proporcionada en el plan del tratamiento deberá incluir:

- Fundamento de la selección de las opciones para el tratamiento, tomando en consideración los beneficios esperados.

- Las medidas del desempeño y de las restricciones.

- Las personas encargadas de la rendición de cuentas, así como las responsables de la aprobación e implementación del plan.

- Todas las acciones propuestas y los recursos necesarios, incluyendo las contingencias.

- Los informes y seguimientos requeridos luego de su implementación.

- Los plazos previstos para la ejecución de las acciones.

En resumen, para que la gestión de riesgo sea eficiente y se cumplan los objetivos planteados, se requiere del compromiso de la Dirección general de la organización, la elaboración de un Plan de Gestión de Seguridad, la asignación de recursos y delegación de funciones y responsabilidades, así como la capacitación del capital humano y- sin olvidar los controles y mejoras constantes.

BIBLIOGRAFÍA

AUDITORÍA DE CÓDIGO. (24 de abril de 2021). El arte del desarrollo seguro (diseño seguro). https://auditoriadecodigo.com/desarrollo-seguro-es-diseno-seguro/

COBB, S. (14 de mayo de 2014). 4 pasos para armar un Plan de Continuidad del Negocio que asegure el futuro digital de la empresa. https://www.welivesecurity.com/la-es/2014/05/14/gestion-continuidad-negocio-cuatro-pasos/

DATAHACK. (12 de noviembre de 2020). LAS 10 V'S DEL BIG DATA. https://www.datahack.es/blog/big-data/10-vs-del-big-data/

ESCUELA EUROPEA DE EXCELENCIA. (16 de mayo de 2018). Cómo realizar la evaluación de riesgos según ISO 31000:2018. https://www.escuelaeuropeaexcelencia.com/2018/05/como-realizar-la-evaluacion-de-riesgos-segun-iso-310002018/#:%7E:text=La%20evaluaci%C3%B3n%20de%20riesgos%20seg%C3%BAn%20ISO%2031000%3A2018%20es%20un,compartir%20o%20tratar%20los%20riesgos

ISACA. (1 de noviembre de 2014). Auditing Oracle Database. https://www.isaca.org/resources/isaca-journal/

past-issues/2014/auditing-oracle-database

ISO 22301. (29 de abril de 2019). Software ISO. https://www.iso-tools.org/normas/riesgos-y-seguridad/iso-22301/

ISO 31000:2018. (2018). Software ISO. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

LÓPEZ, A. (S. F.). ISO 27001. ISO 27000.es. Recuperado 7 de julio de 2021, de https://www.iso27000.es/iso27002_5.html

OCHOA VÁSQUEZ, J. M. (noviembre de 2020). Aplicando data science, análisis de datos e inteligencia artificial a ciberinteligencia. Máster en data science y análisis de datos. Instituto Europeo de Estudios Empresariales.

THOMAS, K. (24 de agosto de 2015). Los usuarios de Ashley Madison, "blancos fáciles para la extorsión". https://www.welivesecurity.com/la-es/2015/08/24/usuarios-ashley-madison-blancos-extorsion/

TRANSFORMING DATA WITH INTELLIGENCE. (8 de febrero de 2017). The 10 Vs of Big Data. https://tdwi.org/articles/2017/02/08/10-vs-of-big-data.aspx

Imágenes de portadas obtenidas de Shutterstock.

ADEN