Valoración del riesgo de ciberseguridad

Breve descripción:

La valoración de riesgos en ciberseguridad en las organizaciones permite determinar el riesgo existente en los activos de información, para que a partir de un ejercicio evaluativo se determinen las salvaguardas necesarias para evitar que las amenazas se materialicen y conlleven a procesos críticos para la organización.

Junio 2023

Tabla de contenido

Introducción

El proceso de valoración del riesgo en los activos de la organización permite determinar el grado de criticidad de estos, frente a una posible amenaza y que a partir de un ejercicio de evaluación aplicando metodologías como la que indica la ISO 31000 o Magerit, se pueden establecer acciones básicas y necesarias para que estas amenazas no se materialicen y afecten el desarrollo de las operaciones de la organización.

A continuación, vamos a revisar algunos temas específicos relacionados con la valoración del riesgo y cómo la podemos aplicar a cualquier organización independientemente de su naturaleza, tamaño o sector económico.

Video 1. Valoración del riesgo de ciberseguridad.

Enlace de reproducción del video

Síntesis del video: Valoración del riesgo de ciberseguridad
Cuando se habla de riesgos informáticos y ciberseguridad se refiere a la identificación de distintas amenazas que afectan, a nivel informático, a una organización. Gestionar los riesgos de manera preventiva nos permite identificar posibles focos de vulnerabilidades y establecer un plan de implementación de salvaguardas que reduzcan su efecto en caso de ser materializadas. Es muy importante tener un control de accesos y controles lógicos orientados a proteger la confidencialidad e integridad de la información, es decir, que no sea revelada a personal no autorizado y que no pueda ser manipulada sin la debida autorización. MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) elaborada por el Consejo Superior de Administración Electrónica, permite estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. La gestión de riesgos es parte fundamental de los procesos para la obtención de registros de acreditación, como los de los sistemas de gestión de la seguridad de la información. Se invita a los aprendices a explorar el material y herramientas para aplicarlos en una correcta valoración de los riesgos.

1. Gestión del riesgo informático

La gestión del riesgo informático se consolida como una práctica que busca a partir de metodologías, identificar oportunamente posibles vulnerabilidades que puedan ser aprovechadas mediante amenazas y evitar que se conviertan en un riesgo y mejor aún, que no se materialicen, evitando incidentes que conlleven a situaciones críticas; esta estrategia ayudar a determinar de manera preventiva cualquiera de estas situaciones y permite identificar los controles y salvaguardas necesarias para hacer frente y evitar que estas situaciones sucedan en las organizaciones.

1.1. Objetivo, características y beneficios

La gestión del riesgo se consolida como un proceso que permite identificar, evaluar y proponer estrategias para enfrentar los riesgos que pueden presentarse ante un activo de información.

Los objetivos, características y beneficios, son:

a) Objetivos

- Reconocer los tipos de riesgos que pueden afectar las operaciones en una organización.
- Evaluar y controlar los riesgos, a partir de la aplicación de salvaguardar.

b) Características

- La gestión del riesgo, debe ser un proceso continuo, nunca termina ni se interrumpe.

- Aplica métodos para la atención de los riesgos identificados.
- Debe ser incorporado dentro de la cultura organizacional.

c) Beneficios

- Optimización del proceso de toma de decisiones.
- Ofrece una visión integrada del negocio.
- Permite aprovechar los recursos.
- Reduce los imprevistos causados por incidentes.
- Permite fortalecer los sistemas de control.

1.2. Etapas

La gestión del riesgo, de acuerdo con las normas específicas como son ISO 31000 o Magerit, establecen etapas que permiten abordar sus métodos para realizar una adecuada gestión del riesgo en las organizaciones a partir de 4 principales etapas. Estas etapas generales, permiten realizar un ejercicio dentro de las organizaciones, que buscan de manera sistemática y organizada, establecer la siguiente ruta:

- **Identificar:** se deben reconocer cada uno de los activos de información para el desarrollo de sus actividades, para que a partir de estos, se puedan identificar las fuentes de riesgo de manera particular a cada uno de los activos; este reconocimiento debe ser riguroso y debe permitir caracterizar el grado de importancia para la misma organización.

- **Evaluar:** una vez identificados los activos de información en la organización, estos deben de evaluar los riesgos, probabilidad de impacto, y la criticidad de estos riesgos y cómo pueden afectar a la organización.
- **Reaccionar:** en esta etapa, se establecerán las acciones necesarias para controlar el riesgo identificado, esto se deberá de plantear mediante un plan de acción, con unos recursos y tiempos establecidos, los cuales deberán ser alcanzables y medibles por la organización.
- **Controlar:** esta etapa conlleva a realizar seguimiento y evaluación de los riesgos, de tal manera que permita identificar el nivel de control que se realiza sobre los mismos, a su vez, permitirá evaluar la efectividad de los controles propuestos con el fin de mejorar o reemplazar los controles establecidos.

En la siguiente figura, se presenta gráficamente, las etapas anteriormente mencionadas.

Figura 1. Etapas evaluación del riesgo

2. Controles de seguridad

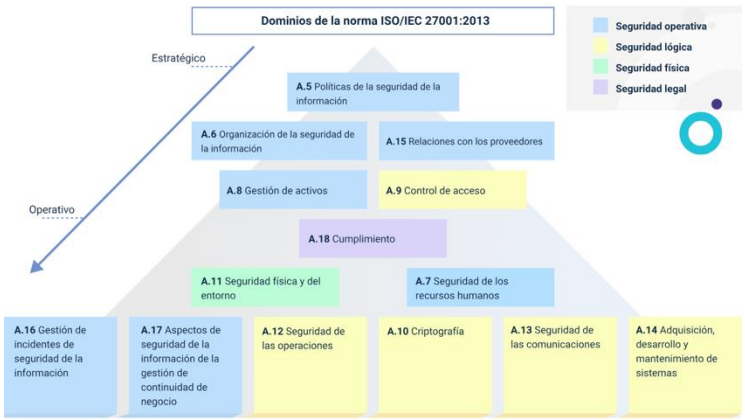
La norma ISO/IEC 27001:2013, como norma fundamental para la implementación de sistemas de gestión de la seguridad de la información, nos propone en su Anexo A, una propuesta de controles bajo un esquema basada en dominios, los cuales tienen enfoque desde lo operativo, lógico, físico y legal, que, a partir de su implementación, permiten controlar las posibles vulnerabilidades que se presentan en las organizaciones.

Los controles de seguridad se recomiendan sean implementados a partir del análisis de riesgos, esto permitirá hacer frente de manera asertiva a las necesidades identificadas en cada uno de los activos de información.

Dominios

Los controles que nos propone la norma ISO/IEC 27001:2013 en su anexo A, corresponden a las categorías y/o aspectos que deben ser abordados desde la estrategia de seguridad propuesta para contar con un nivel mínimo de resistencia ante cualquier riesgo, como se muestra en la siguiente figura.

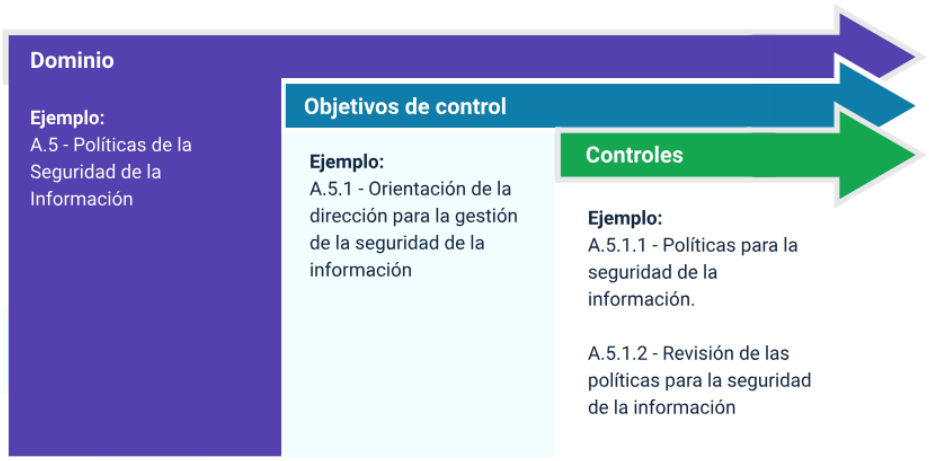
Figura 2. Dominios de seguridad de la norma ISO/IEC 27001:2013



Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

Estas categorías están clasificadas desde la A.5 hasta el A.18, que corresponden a 14 dominios que representan los niveles de seguridad como son: operativos, lógicos, físicos y legales; los cuales se pueden identificar desde el ámbito estratégico al igual que operativo. Lo anterior se puede observar en la figura No. 3.

Figura 3. Ejemplo de dominio de la norma ISO/IEC 27001:2013



Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

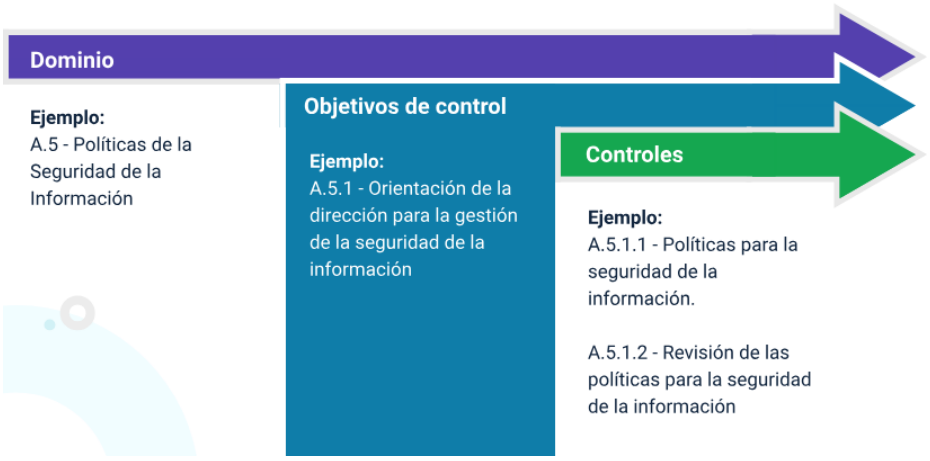
Un ejemplo de dominio de la norma ISO/IEC 27001:2013 es el A.5 – Políticas de la Seguridad de la Información.

Estos dominios permiten reconocer cada uno de los ámbitos de aplicación y administración, los cuales necesariamente deben ser tenidos en cuenta, estos 4 ámbitos son abordados desde la óptica de la organización y de acuerdo con sus necesidades, activos de información, relación con terceros y desde el análisis de riesgo que se debe realizar.

Objetivos de control

Cada uno de los dominios de seguridad que nos presenta la norma ISO/IEC 27001:2013 descritos anteriormente, se encuentra divididos en categorías denominadas Objetivos de control el cual nos brinda las políticas principales de los controles de seguridad que se implementarán, revise la siguiente figura, que muestra información al respecto.

Figura 4. Objetivo de control de la norma ISO/IEC 27001:2013



Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

Para el ejemplo que venimos trabajando: Dominio A.5 – Políticas de la Seguridad de la Información, tenemos que los objetivos de control son: A.5.1 – Orientación de la dirección para la gestión de la seguridad de la información.

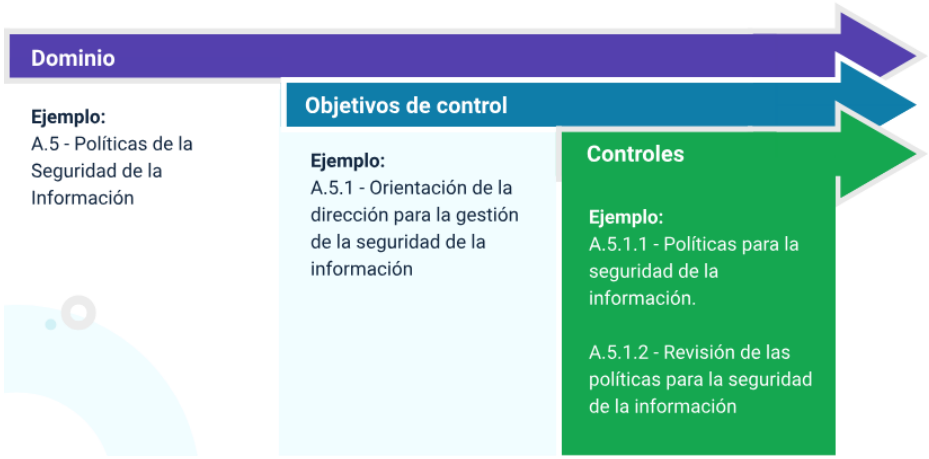
Estos objetivos de control como su nombre lo indica, representa aquello que se busca obtener con la aplicación de los controles de seguridad, de tal manera que, en un ejercicio de aplicación, su adopción corresponde a las necesidades y problemas que la organización quiere abordar.

2.1. Controles

Los controles, se presentan como las propuestas y directrices para la implementación de una estrategia de seguridad, que puede ir desde el endurecimiento de la infraestructura hasta la consolidación de un sistema de gestión de la seguridad SGSI, con los cuales se busca garantizar los objetivos de seguridad de la organización.

En este orden de ideas, la estructura de los objetivos de control se presenta de acuerdo con la figura 5, en donde encontramos la idea principal, plasmada de manera general, acompañada de una descripción de la utilidad de este.

Figura 5. Ejemplo de controles de la norma ISO/IEC 27001:2013



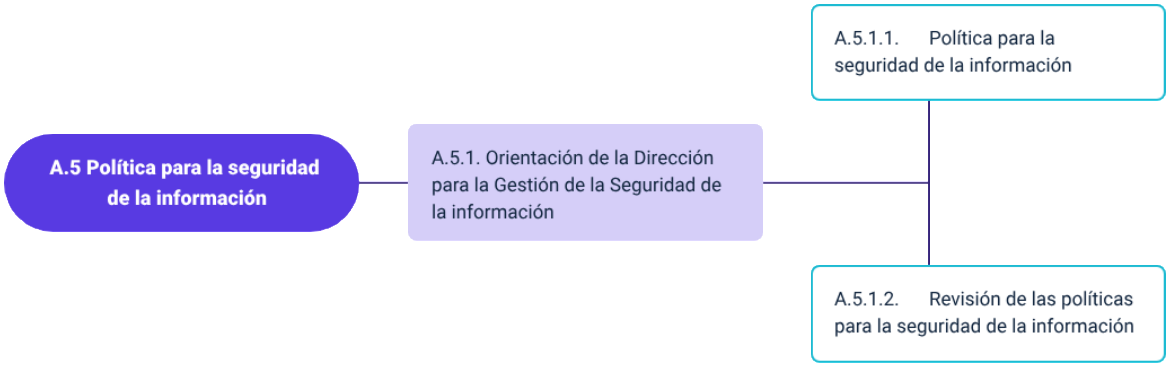
Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

Continuando con el ejemplo, tenemos que el dominio es: A.5 – Políticas de la Seguridad de la Información, los objetivos de control: A.5.1 – Orientación de la dirección para la gestión de la seguridad de la información, y finalmente los controles son: A.5.1.1 – Políticas para la seguridad de la información y A.5.1.2 – Revisión de las políticas para la seguridad de la información.

Los dominios de seguridad que propone esta norma se encuentran estructurados de acuerdo con los componentes y elementos más relevantes para el mejoramiento de los activos de información y estos proponen los siguientes objetivos de control:

En una organización se deben de gestionar los activos de información de manera segura y responsable, por ello la norma nos recomienda que se cuente con políticas claras que apoyen el ejercicio de identificación y aseguramiento de los activos de la información. En la siguiente figura, podremos encontrar los objetivos de control para la determinación de estas políticas.

Figura 6. A.5 Política para la seguridad de la información



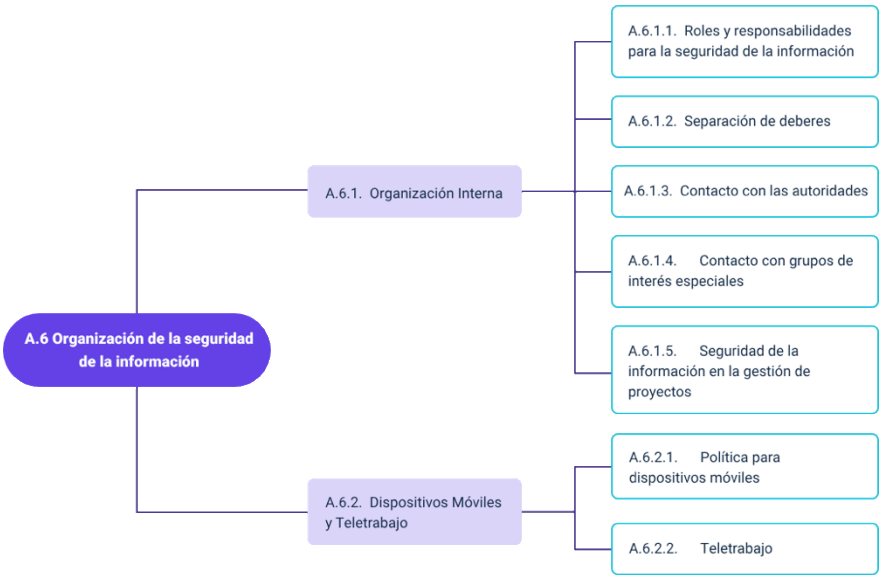
Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

La política para la seguridad de la información (A.5), se compone de la orientación de la dirección para la gestión de la seguridad de la información (A.5.1) y esta a su vez de la política para la seguridad de la información (A.5.1.1) y la revisión de las políticas para la seguridad de la información (A.5.1.2).

Uno de los factores importantes en una organización es brindar las directrices para identificar y mantener seguros los activos de información, en la figura No. 7,

podremos consultar los objetivos de control para la organización de la seguridad de la información.

Figura 7. A.6 Organización de la seguridad de la información



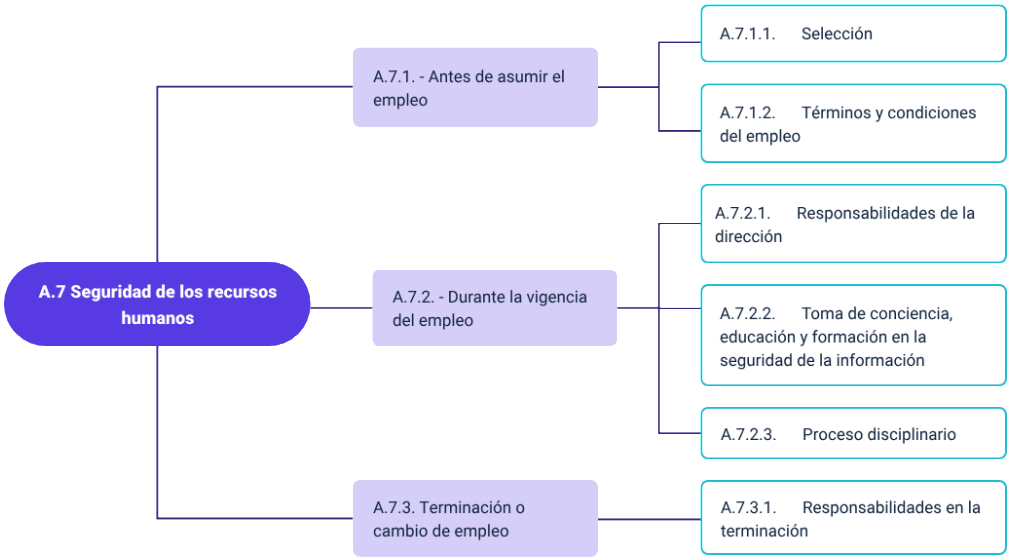
Nota: Adaptada de ISO/IEC 27001:2013 – Anexo A.

La organización de la seguridad de la información (A.6), está compuesta por:

- La organización interna (A.6.1.): la componen los roles y responsabilidades para la seguridad de la información (A.6.1.1.), la separación de deberes (A.6.1.2.), el contacto con las autoridades (A.6.1.3.), el contacto con grupos de interés especiales (A.6.1.4.) y la seguridad de la información en la gestión de los proyectos (A.6.1.5.).
- Los dispositivos móviles y teletrabajo (A.6.2.): lo componen la política para dispositivos móviles (A.6.2.1.) y el teletrabajo (A.6.2.2.).

Uno de los factores más débiles en seguridad será el factor humano, de acuerdo con el instituto internacional de estudios en seguridad global “El error humano es la principal causa de infracciones de datos y no los ciberdelincuentes. Es aquí donde las compañías deben revisar sus protocolos” (INISEG, 2020). Para abordar estos factores humanos, la norma nos presenta en la figura No. 8 los siguientes objetivos de control.

Figura 8. A.7 Seguridad de los recursos humanos



Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

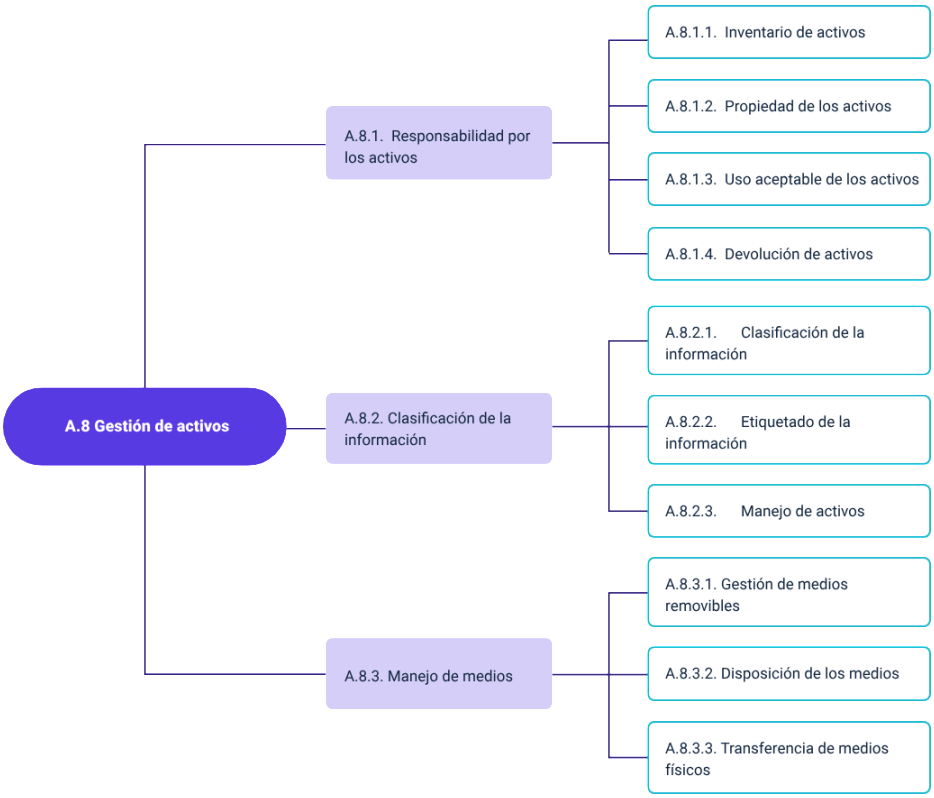
La seguridad de los recursos humanos (A.7) comprende:

- Antes de asumir el empleo (A.7.1.): se compone de la selección (A.7.1.1.) y los términos y condiciones del empleo (A.7.1.2.).
- Durante la vigencia del empleo (A.7.2.): se compone de las responsabilidades de la dirección (A.7.2.1.), la toma de conciencia, educación y formación en la seguridad de la información (A.7.2.2.) y el proceso disciplinario (A.7.2.3.).

- Terminación o cambio de empleo (A.7.3.): se compone de las responsabilidades en la terminación (A.7.3.1.).

La gestión de activos de información cobra vital importancia dado que estos deben mantenerse identificados, clasificados y salvaguardados; en la figura No. 9 encontramos los objetivos de control que establecen los controles necesarios para gestionar estos activos.

Figura 9. A.8 Gestión de activos



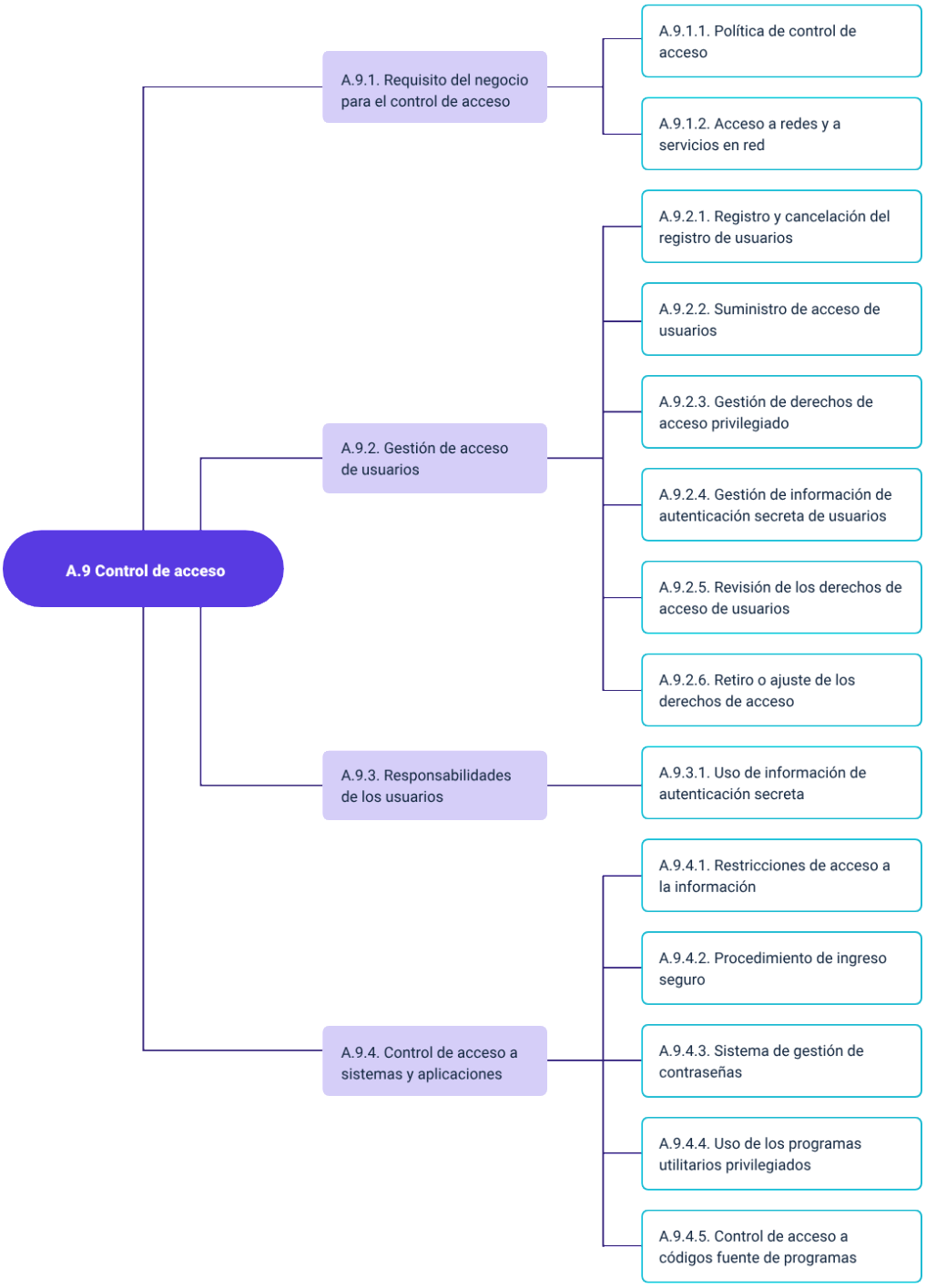
Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

La gestión de archivos (A.8) comprende:

- La responsabilidad por los activos (A.8.1.): se compone del inventario de activos (A.8.1.1.), la propiedad de los activos (A.8.1.2.), el uso aceptable de los activos (A.8.1.3.) y la devolución de activos (A.8.1.4.).
- La clasificación de la información (A.8.2.): se compone de la clasificación de la información (A.8.2.1.), el etiquetado de la información (A.8.2.2.) y el manejo de activos (A.8.2.3.).
- El manejo de medios (A.8.3.): se compone de la gestión de medios removibles (A.8.3.1.), la disposición de los medios (A.8.3.2.) y la transferencia de medios físicos (A.8.3.3.)

Otro factor importante es la restricción al acceso a los activos de información, a continuación, en la figura No. 10 podremos encontrar los controles para gestionar estos accesos, prevaleciendo siempre la confidencialidad, privacidad y disponibilidad del activo de información.

Figura 10. A.9 Control de acceso



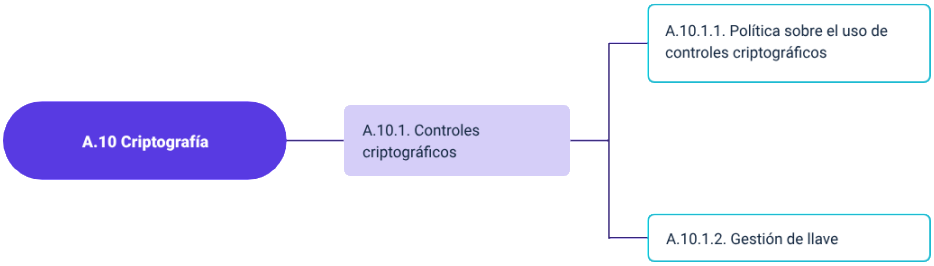
Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

El control de acceso (A.9) comprende:

- El requisito del negocio para el control de acceso (A.9.1.): se compone de la política de control de acceso (A.9.1.1.) y el acceso a redes y servicio en red (A.9.1.2.).
- La gestión de acceso de usuarios (A.9.2.): se compone del registro y cancelación del registro de usuarios (A.9.2.1.), el suministro de acceso de usuarios (A.9.2.2.), la gestión de derechos de acceso privilegiado (A.9.2.3.), la gestión de información de autenticación secreta de usuarios (A.9.2.4.), la revisión de los derechos de acceso de usuarios (A.9.2.5.) y el retiro o ajuste de los derechos de acceso (A.9.2.6.).
- Las responsabilidades de los usuarios (A.9.3.): se compone del uso de información de autenticación secreta.
- El control de acceso a sistemas y aplicaciones (A.9.4.): se compone de las restricciones de acceso a la información (A.9.4.1.), el procedimiento de ingreso seguro (A.9.4.2.), el sistema de gestión de contraseñas (A.9.4.3.), el uso de los programas utilitarios privilegiados (A.9.4.4.) y el control de acceso a códigos fuente de programas (A.9.4.5.).

Para proteger la información de ser accedida por personas o sistemas no autorizados, se recomienda el uso de sistemas y técnicas de criptografía con el fin de garantizar la confidencialidad e integridad de estos, en la figura No. 11 podremos encontrar los controles sugeridos por la norma.

Figura 11. A.10 Criptografía

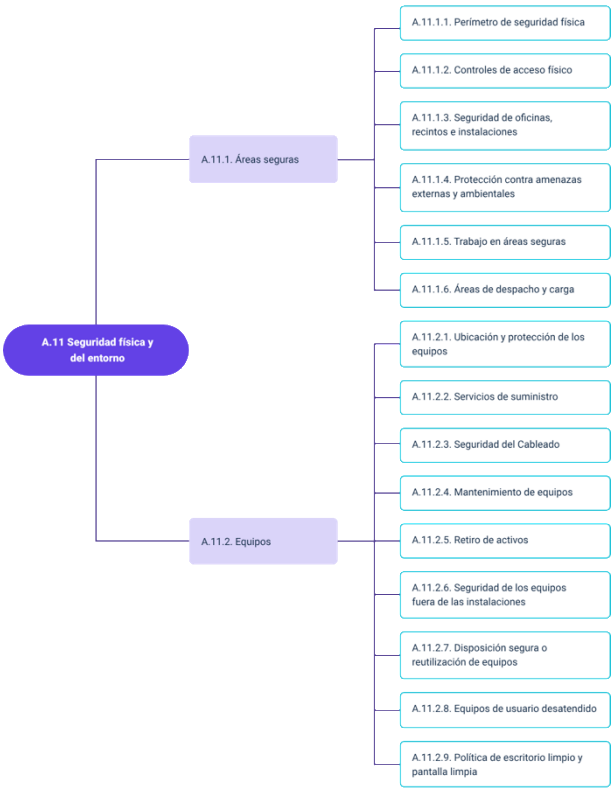


Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

La criptografía (A.10) comprende los controles criptográficos (A.10.1.), el cual se compone de la política sobre el uso de controles criptográficos (A.10.1.1.) y la gestión de la llave (A.10.1.2.).

Como buenas prácticas de seguridad, se recomienda reducir los riesgos asociados por daños directos o factores que puedan afectar los activos de información o el desarrollo de las operaciones en la organización, a continuación, en la figura No. 12, podremos encontrar los controles sugeridos para el aseguramiento físico como del entorno en donde se encuentran ubicados dichos activos.

Figura 12. A.11 Seguridad física y del entorno



Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

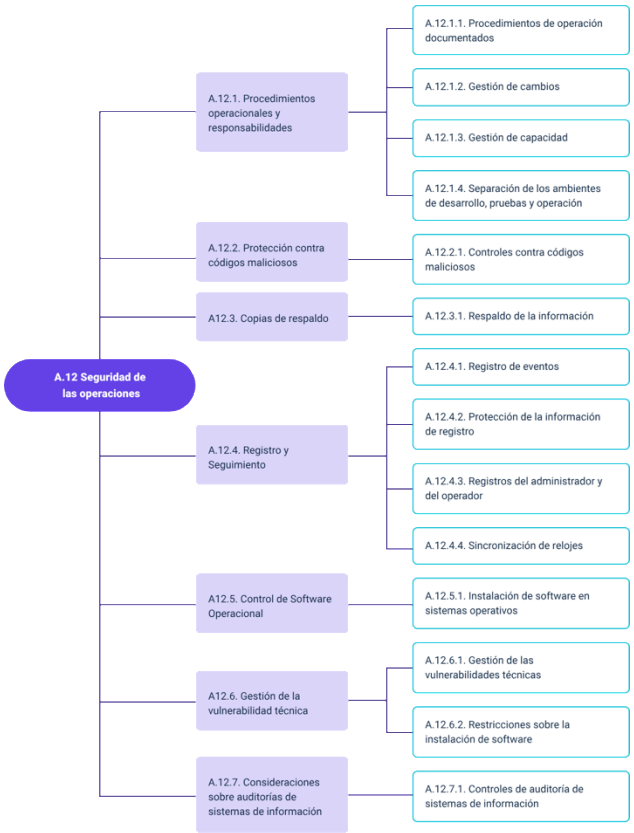
La seguridad física y del entorno (A.11) comprende:

- Las áreas seguras (A.11.1.): se componen del perímetro de seguridad física (A.11.1.1.), los controles de acceso físico (A.11.1.2.), la seguridad de oficinas, recintos e instalaciones (A.11.1.3.), la protección contra amenazas externas y ambientales (A.11.1.4), el trabajo en áreas seguras (A.11.1.5.) y las áreas de despacho y carga (A.11.1.6.).
- Los equipos (A.11.2.): se componen de la ubicación y protección de los equipos (A.11.2.1.), los servicios de suministro (A.11.2.2.), la seguridad del cableado (A.11.2.3.), el mantenimiento de equipos (A.11.2.4.), el retiro de

activos (A.11.2.5.), la seguridad de los equipos fuera de las instalaciones (A.11.2.6), la disposición segura o reutilización de equipos (A.11.2.7), los equipos de usuario desatendido (A.11.2.8) y la política de escritorio limpio y pantalla limpia (A.11.2.9).

El riesgo de que una organización sea afectada por un incidente es permanente, cada día se presentan nuevas amenazas que pueden interrumpir o dañar los activos de información de la organización, por ello, en la figura No. 13 se presentan algunos controles sugeridos para reducir este tipo de riesgos.

Figura 13. A.12 Seguridad de las operaciones



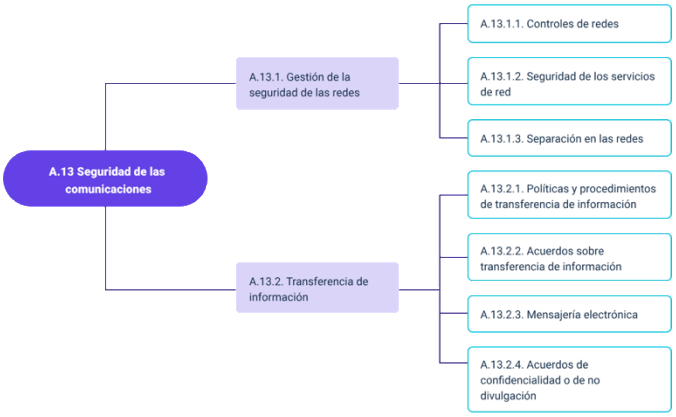
Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

La seguridad de las operaciones (A.12) comprende:

- Los procedimientos operacionales y responsabilidades (A.12.1.): se componen de los procedimientos de operación documentados (A.12.1.1.), la gestión de cambios (A.12.1.2.), la gestión de capacidad (A.12.1.3.) y la separación de los ambientes de desarrollo, pruebas y operación (A.12.1.4.).
- La protección contra códigos maliciosos (A.12.2.): se compone de los controles contra códigos maliciosos (A.12.2.1.).
- Las copias de respaldo (A.12.3.): se compone del respaldo de la información (A.12.3.1.).
- El registro y seguimiento (A.12.4.): se compone del registro de eventos (A.12.4.1.), la protección de la información de registro (A.12.4.2.), los registros del administrador y del operador (A.12.4.3.) y la sincronización de relojes (A.12.4.4.).
- El control de "software" operacional (A.12.5.): se compone de la instalación de "software" en sistemas operativos (A.12.5.1.).
- La gestión de la vulnerabilidad técnica (A.12.6.): se compone de la gestión de las vulnerabilidades técnicas (A.12.6.1.) y las restricciones sobre la instalación de "software" (A.12.6.2.).
- Las consideraciones sobre auditorías de sistemas de información (A.12.7.): se compone de los controles de auditoría de sistemas de información (A.12.7.1.).

Otro factor importante hoy en día, es la transmisión e intercambio de información, por ello en la figura No. 14, se presentan algunos controles que nos permiten gestionar la seguridad en las redes, así como en el proceso de transferencia e intercambio de información.

Figura 14. A.13 Seguridad de las comunicaciones



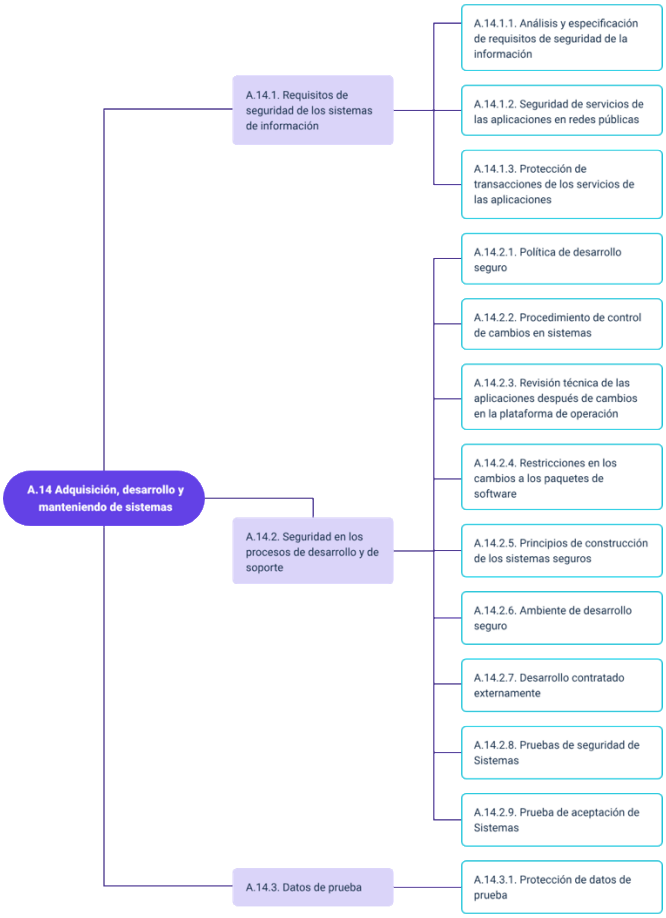
Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

La seguridad de las comunicaciones (A.13) comprende:

- La gestión de la seguridad de las redes (A.13.1.): se compone de los controles de redes (A.13.1.1.), la seguridad de los servicios de red (A.13.1.2.) y la separación de las redes (A.13.1.3.).
- La transferencia de información (A.13.2.): se compone de las políticas y procedimientos de transferencia de información (A.13.2.1.), los acuerdos sobre transferencia de información (A.13.2.2.), la mensajería electrónica (A.13.2.3.) y los acuerdos de confidencialidad o de no divulgación (A.13.2.4.).

Actualmente, las organizaciones cuentan con departamentos o grupos encargados de desarrollar y mantener sus propias soluciones, en la figura No. 15, podemos encontrar controles que deben ser tenidos en cuenta en este tipo de actividades.

Figura 15. A.14 Adquisición, desarrollo y manteniendo de sistemas



Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

La adquisición, desarrollo y mantenimiento de sistemas (A.14) comprende:

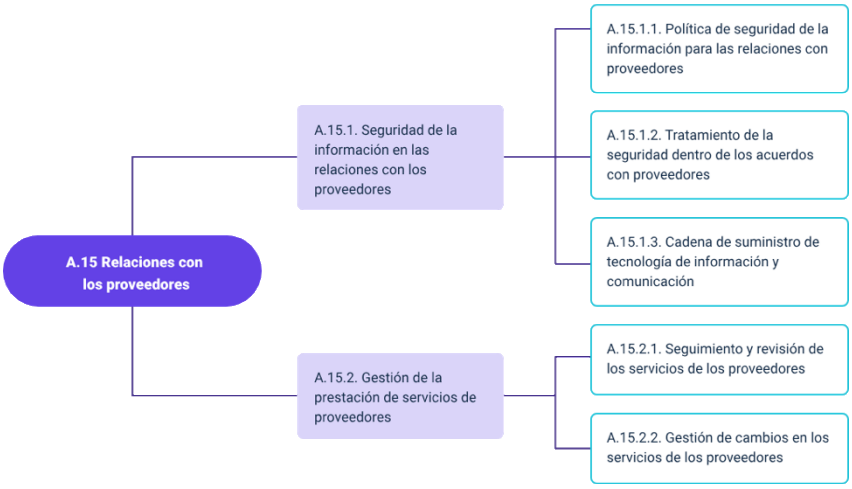
- Los requisitos de seguridad de los sistemas de información (A.14.1.): se componen del análisis y especificación de requisitos de seguridad de la

información (A.14.1.1.), la seguridad de servicios de las aplicaciones en redes públicas (A.14.1.2.) y la protección de transacciones de los servicios de las aplicaciones.

- La seguridad en los procesos de desarrollo y de soporte (A.14.2.): se compone de la política de desarrollo seguro (A.14.2.1.), el procedimiento de control de cambios en sistemas (A.14.2.2.), la revisión técnica de las aplicaciones después de cambios en la plataforma de operación (A.14.2.3.), las restricciones en los cambios a los paquetes de "software" (A.14.2.4.), los principios de construcción de los sistemas seguros (A.14.2.5.), el ambiente de desarrollo seguro (A.14.2.6.), el desarrollo contratado externamente (A.14.2.7.), las pruebas de seguridad de sistemas (A.14.2.8.) y la prueba de aceptación de sistemas (A.14.2.9.)
- Los datos de prueba (A.14.3.): se compone de la protección de datos de prueba (A.14.3.1.)

La relación con los proveedores de productos o servicios en la organización, debe estar alineada con las políticas de seguridad, y para este caso, en la figura No. 16 encontramos algunos controles sugeridos para asegurar un apropiado intercambio de información con sus proveedores.

Figura 16. A.15 Relaciones con los proveedores



Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

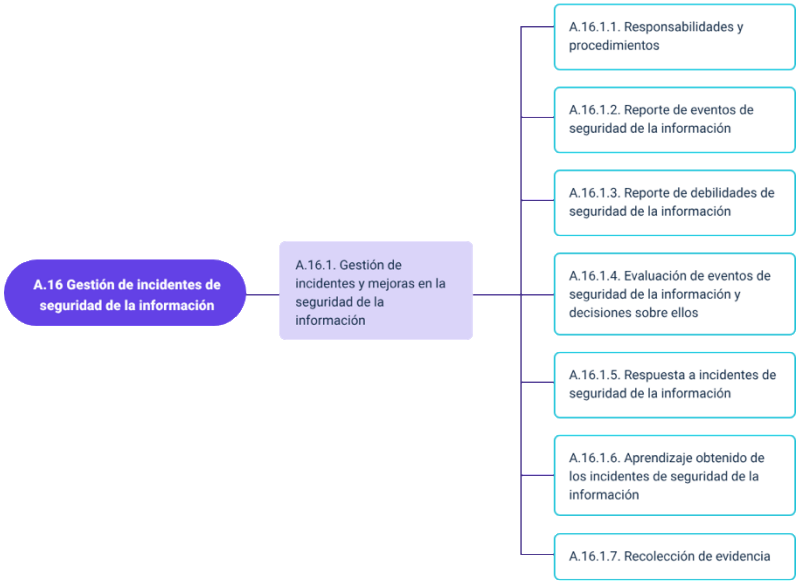
Las relaciones con los proveedores (A.15) comprenden:

- La seguridad de la información en las relaciones con los proveedores (A.15.1.): se compone de la política de seguridad de la información para las relaciones con proveedores (A.15.1.1.), el tratamiento de la seguridad dentro de los acuerdos con proveedores (A.15.1.2.) y la cadena de suministro de tecnología de información y comunicación (A.15.1.3.).
- La gestión de la prestación de servicios de proveedores (A.15.2.): comprende el seguimiento y revisión de los servicios de los proveedores (A.15.2.1.) y la gestión de cambios en los servicios de los proveedores (A.15.2.2.).

Cualquier organización está sujeta a sufrir algún incidente de seguridad que afecte el desarrollo de sus funciones, a continuación, en la figura No. 17 encontramos

algunos controles sugeridos para gestionar este tipo de incidentes y recuperarse lo más rápido posible.

Figura 17. A.16 Gestión de incidentes de seguridad de la información



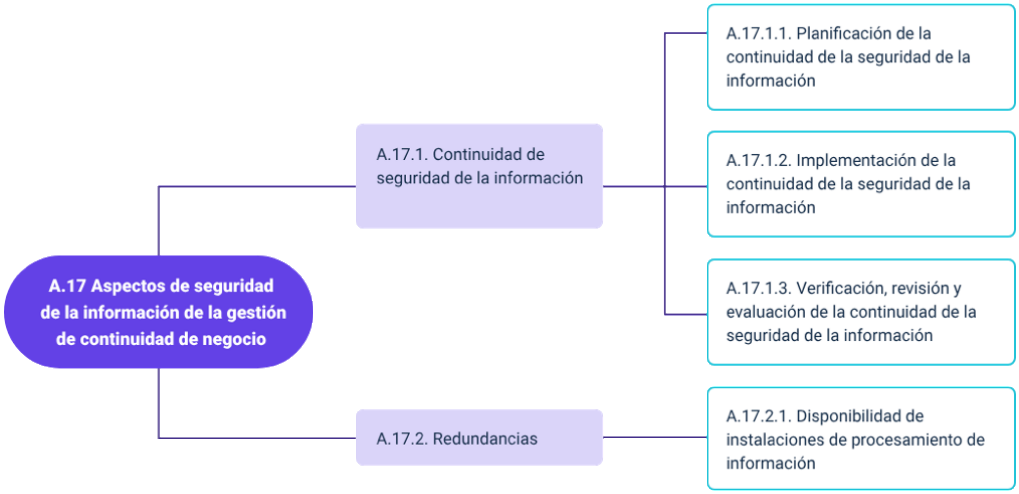
Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

La gestión de incidentes de seguridad de la información (A.16) comprende la gestión de incidentes y mejoras en la seguridad de la información (A.16.1.), la cual se compone de las responsabilidades y procedimientos (A.16.1.1.), el reporte de eventos de seguridad de la información (A.16.1.2.), el reporte de debilidades de seguridad de la información (A.16.1.3.), la evaluación de eventos de seguridad de la información y decisiones sobre ellos ((A.16.1.4.), la respuesta a incidentes de seguridad de la información (A.16.1.5.), el aprendizaje obtenido de los incidentes de seguridad de la información (A.16.1.6.) y la recolección de evidencia (A.16.1.7.).

Garantizar la continuidad del negocio es un factor importante tras sufrir un incidente, por ello se presentan en la figura No. 18, los controles que garanticen que la

organización podrá recuperarse en un mínimo tiempo, con una mínima pérdida de información.

Figura 18. A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio



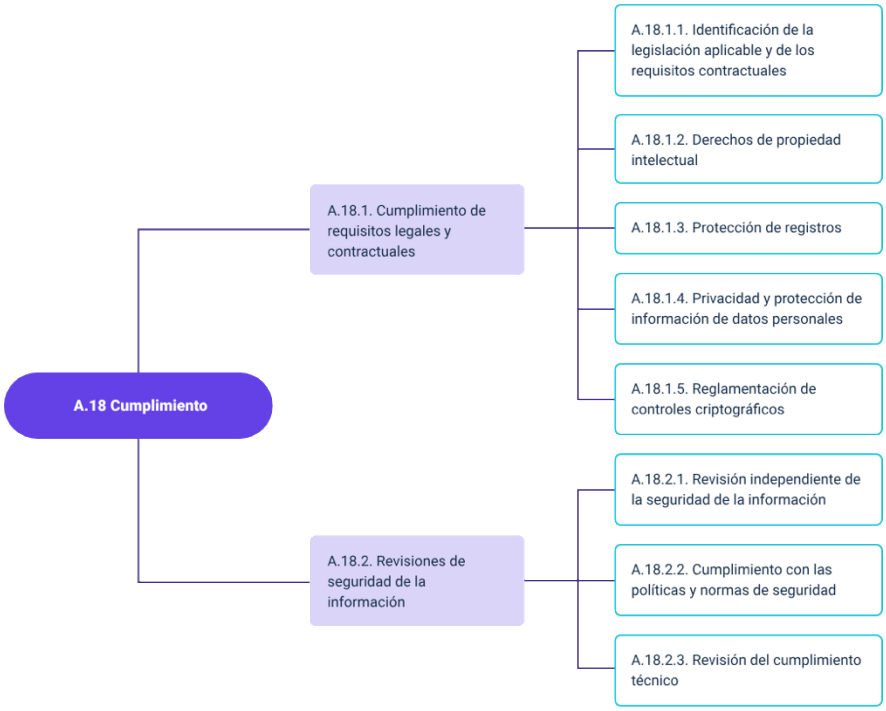
Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

Los aspectos de seguridad de la información de la gestión de continuidad de negocio (A.17) comprende:

- La continuidad de seguridad de la información (A.17.1.): se compone de la planificación de la continuidad de la seguridad de la información (A.17.1.1.), la implementación de la continuidad de la seguridad de la información (A.17.1.2.) y la verificación, revisión y evaluación de la continuidad de la seguridad de la información (A.17.1.3.).
- Las redundancias (A.17.2.): se componen de la disponibilidad de instalaciones de procesamiento de información (A.17.2.1.)

Finalmente, el cumplimiento de los requisitos legales garantiza el actuar de la organización, y evitan incurrir en alguna falta que afecte en un futuro la organización, por ello, en la figura No. 19 se presentan los controles de cumplimiento que buscan reducir los riesgos al incurrir en una falta relacionada.

Figura 19. A.18 Cumplimiento



Nota. Adaptada de ISO/IEC 27001:2013 – Anexo A.

El cumplimiento (A.18) comprende:

- El cumplimiento de los requisitos legales y contractuales (A.18.1.): se compone de la identificación de la legislación aplicable y de los requisitos contractuales (A.18.1.1.), los derechos de propiedad intelectual (A.18.1.2.), la protección de registros (A.18.1.3.), la privacidad y protección de

información de datos personales (A.18.1.4.) y la reglamentación de controles criptográficos (A.18.1.5.).

- Las revisiones de seguridad de la información (A.18.2.): se componen de la revisión independiente de la seguridad de la información (A.18.2.1.), el cumplimiento con las políticas y normas de seguridad (A.18.2.2.) y la revisión del cumplimiento técnico (A.18.2.3.).

Estos objetivos de control en profundidad pueden ser consultados en la Norma ISO/IEC 27001:2013 – Anexo A para identificar aspectos más en profundidad sobre los controles de seguridad.

2.2. Declaración de aplicabilidad

Esta Declaración de Aplicabilidad o también conocido como "Statement of Applicability" (SoA), es un instrumento que consolida la relación completa de controles sugeridos por la Norma ISO/IEC 27001:2013, para la implementación de estrategias de seguridad, y sirve para presentar el detalle de aquellos controles que serán adoptados por la organización.

Este documento es construido desde el ejercicio de análisis de riesgos, por lo que se considera un documento de referencia tanto para la implementación de controles, así como para la evaluación de la eficacia de estos a futuro.

En la tabla 1, podemos observar un ejemplo de documento de Declaración de Aplicabilidad, en donde se establecen los controles, su aplicación, su justificación, responsable, así como el plan de acción a realizar para su implementación.

Tabla 1. Ejemplo de documento de Declaración de Aplicabilidad SoA

A.5.1 Orientación de la Dirección para la Gestión de la Seguridad de la información: brindar orientación y soporte, por parte de la Dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

N°	Dominio – Control general	Descripción del control (consulta la norma de declaración de aplicabilidad Anexo A ISO 270012013)	Aplica Sí/No	Justificación	Responsabilidad	Plan de acción
A.5.1.1	Política para la seguridad de la información.	La dirección debe aprobar, publicar y comunicar a todos los empleados y partes externas pertinentes, un documento de política de seguridad de la información.	Sí	El contar con la política de seguridad de la información de un punto de partida para la implementación en la organización.	Alta gerencia.	La alta dirección de la Superintendencia de Sociedades aprobó la política de gestión integral y se ha comunicado a todos los funcionarios y las partes externas pertinentes a través de correo electrónico, intranet e internet.

N°	Dominio – Control general	Descripción del control (consulta la norma de declaración de aplicabilidad Anexo A ISO 270012013)	Aplica Sí/No	Justificación	Responsabilidad	Plan de acción
A.5.1.2	Revisión de las políticas para la seguridad de la información.	Se debe revisar la política de seguridad de la información a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, suficiencia y eficacia continuas.	Sí	De acuerdo con el ciclo PHVA se debe programar periodos de evaluación de la política de seguridad de la información la cual permite implementar mejoras permanentes.	Alta gerencia.	La alta dirección de la Superintendencia de Sociedades realiza a intervalos planificados la revisión al sistema de gestión integrado en el proceso de gestión estratégica donde las salidas reflejan cambios a la política de gestión integral.

Nota. Tomado de https://cutt.ly/GB7xJM9

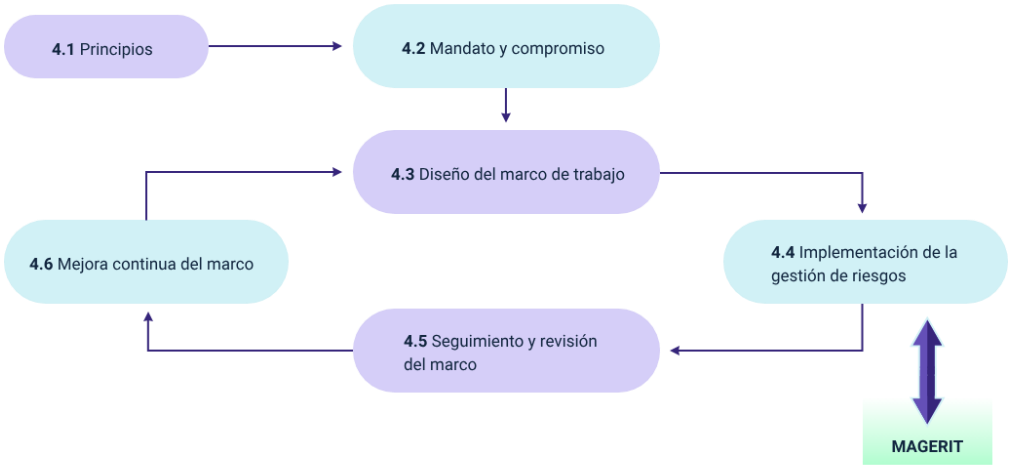
Para el establecimiento de la declaración de aplicabilidad en una organización, esta debe ser diligenciada en su totalidad, realizando el registro de todos y cada uno de los controles establecidos por la norma, indicando cuáles serán aplicables en la organización, cuáles no y su razón de no aplicabilidad, así como la forma en que será

aplicable hacia los activos de información, de esta manera permitirá a las partes interesadas identificar los controles que serán aplicados y evaluados.

3. Magerit

Magerit, se presenta como una metodología para la gestión del riesgo, la cual está basada en la norma ISO 31000, precisamente en su apartado 4.4 denominado Implementar la Gestión del Riesgo, lo que la consolida como un marco para su gestión, como lo presenta la misma metodología en la figura No 20.

Figura 20. Marco de trabajo para la gestión de riesgos de acuerdo con ISO 31000.



Nota. Adaptado de MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

El marco de trabajo para la gestión de riesgos, de acuerdo con ISO 31000, comienza con los principios, luego el mandato y compromiso, pasa a la implementación de la gestión de riesgos, luego viene el seguimiento y revisión del marco y finalmente la mejora continua del marco, para regresar al diseño del marco de trabajo.

Las propuestas normativas buscan identificar el nivel de vulnerabilidad de los activos de información, siendo Magerit preferida por su sencillez y su objetividad en el

momento de su aplicación para la evaluación del riesgo. A continuación, se exponen los objetivos de MAGERIT:

- Busca con su aplicación mejorar la concienciación de la existencia de riesgos.
- Importancia de realizar una adecuada gestión.
- Ofrece un modelo su análisis.
- Determinar las rutas para su gestión.
- Ayuda a las organizaciones con la evaluación de la seguridad en las mismas.

A partir de las siguientes dimensiones de seguridad, se debe realizar la valoración en cada uno de los activos para proceder con el ejercicio de análisis de riesgo, así:

Video 2. Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información).

Enlace de reproducción del video

Síntesis del video: Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)
Magerit permite estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. Disponibilidad: capacidad de disponer de los servicios, cuando sea necesario. Su carencia supone una interrupción al servicio, la disponibilidad afecta directamente a la productividad de las organizaciones. Integridad: capacidad de mantener un dato o activo de información de manera completa y sin modificaciones indebidas.

Confidencialidad: los activos de información sean consultados o lleguen a las personas autorizadas, en contra de la confidencialidad, puede representarse como fugas, filtraciones, así como accesos no autorizados.

Autenticidad: capacidad de identificar si una entidad o usuario es quien dice ser, o que garantiza la fuente u origen de los datos.

Trazabilidad: capacidad de identificar en cualquier momento las condiciones bajo las cuales se realizó alguna acción.

El procedimiento de análisis de riesgos se puede desarrollar en cualquier tipo de organización que desarrolle sus funciones apoyado en sistemas de información y comunicaciones, independiente del sector bien sea público o privado, y se recomienda realizarlo con mayor razón cuando se manejan datos confidenciales.

Los pasos generales para desarrollar un análisis de riesgos, relacionados con la seguridad informática, se evidencian en el siguiente video titulado Procedimiento de Análisis de Riesgos - Pasos:

Video 3. Procedimiento de Análisis de Riesgos - Pasos.

Enlace de reproducción del video

Síntesis del video: Procedimiento de Análisis de Riesgos - Pasos
Los pasos para el procedimiento de análisis de riesgos, son: Identificar activos de la organización: recursos que utiliza un Sistema de Gestión de Seguridad de la Información. Es decir, todo elemento que compone el proceso completo de comunicación, partiendo desde la información, el emisor, el medio de transmisión y receptor.

Reconocimiento de amenazas: es la defensa ante los ciberataques de la información, teniendo en cuenta que la seguridad de una organización depende de una rápida identificación y acciones de respuesta.

Establecimiento de salvaguardas: medidas de seguridad esenciales para reducir el riesgo de ataques al mínimo, midiendo la resistencia del ataque directo y se mide la fuerza que tiene que utilizar el agente agresor.

Establecimiento del impacto de las amenazas: Los mecanismos que utiliza la seguridad de red son: antivirus y "antispyware", cortafuegos, redes privadas para garantizar un acceso seguro a la red y sistemas de prevención de intrusiones (IPS) para identificar amenazas, como la protección "firewall".

Estimación del riesgo: se evalúa mediante la medición de los dos parámetros que lo determinan, la magnitud de la pérdida o daño posible, y la probabilidad que dicha pérdida o daño llegue a ocurrir.

3.1. Identificación de activos

Se debe tener en cuenta que se deben identificar los activos relacionados con los procesos de negocio, que se deben proteger, teniendo en cuenta los elementos de un sistema de información.

La identificación permite clasificar los activos a los que se les debe brindar mayor protección, así:

Figura 21. Identificación de archivos

La identificación de activos comprende:

- **Información propia:** se compone de datos, servicios, aplicaciones informáticas, soportes de información, equipamiento auxiliar, redes de comunicaciones, instalaciones y personas.
- **Información de terceros.**

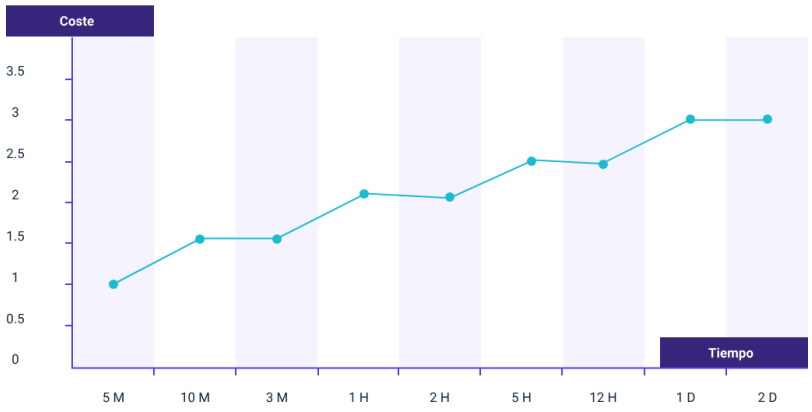
También se establecen las escalas de medición cualitativa y cuantitativa, las cuales se exponen a continuación:

- **Valoración cualitativa:** es un proceso que permite analizar las características y problemas del fenómeno a evaluar permitiendo identificar rápidamente el peso de cada activo en comparación a los demás.
- **Valoración cuantitativa:** estas valoraciones, se presentan en escalas numéricas absolutas las cuales son algo complejas de identificar; pero permiten establecer operaciones matemáticas para sus evaluaciones.

Un último elemento a tener presente en la caracterización de los activos es el valor de la interrupción del servicio, debido a que esta valoración se diferencia de las

anteriores porque afecta directamente la disponibilidad, y se requiere determinar el costo de tenerlo por fuera de servicio por un determinado tiempo; esta valoración se debe establecer en una línea de tiempo que permita identificar claramente las consecuencias de no contar con un sistema de información disponible y su impacto para la organización, por lo general se presentan en gráficos como el que se presenta en la figura a continuación:

Figura 22. Coste de interrupción de la disponibilidad.



Se presenta el coste de interrupción de la disponibilidad, donde el eje X es representado por el tiempo y el eje Y por el coste.

Los anteriores criterios son necesarios para identificar y caracterizar cada uno de los activos de la organización, para continuar con la identificación de amenazas para cada uno de estos.

3.2. Identificación de amenazas

La metodología Magerit, permite identificar las amenazas de cada uno de los activos de información en la organización, para lo cual, nos sugiere una serie de amenazas “típicas”, que mostramos a continuación:

- **Natural:** todos los eventos que origina la naturaleza y puede afectar un activo de información, como desastres naturales, incendios accidentales, tormentas, temperaturas extremas, terremotos e inundaciones, y amenazas ocasionadas por el hombre.

- **Industrial:** generados por efectos resultantes o asociadas a eventos industriales; cualquier empresa con operaciones industriales digitalizadas es susceptible de ser atacada, las más afectadas son las proveedoras de electricidad, agua, petróleo y gas, las alimentarias y las farmacéuticas.

- **Errores en las aplicaciones:** vulnerabilidades técnicas en programas, normalmente se presentan por errores de código, fallas en el diseño de “software”, problemas en la implementación o malas prácticas de configuración de activos.

- **Causados de forma accidental**: originados por personas generalmente por error u omisión, pueden ser errores sistemáticos y errores accidentales.

- **Causadas por las personas de forma deliberada:** según el Artículo 269D: Daño Informático, el que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes, o componentes lógicos causados por terceros, o por personas con intereses propios.

- **Identificación y tipificación de activos:** una vez se haya realizado la identificación de las amenazas, se procede a realizar la valoración de estas, y se requiere identificar cuál sería el efecto de influencia sobre el activo.
- **Degradación**: la degradación mide el daño causado por un incidente en el supuesto de que ocurriera, y esta se suele caracterizar como una fracción del valor del activo y da origen a expresiones como “activo totalmente degradado” o “degradado” en una pequeña fracción.
- **Probabilidad:** qué tan probable es que una amenaza sea aprovechada y se materialice en un riesgo.

La complejidad de ocurrencia es compleja de determinar y expresar, y se puede apoyar en escalas de tipo nominal, como se muestra en la siguiente tabla:

Tabla 2. Ejemplo de escala de degradación del valor por probabilidad de ocurrencia

MA	A	M	B	MB
Muy alta	Alta	Media	Baja	Muy baja
Casi seguro	Muy alto	Posible	Poco probable	Muy raro
Fácil	Medio	Difícil	Muy difícil	Extremadamente difícil

Nota. MAGERIT– versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Ahora bien, en término de periodo de tiempo, lo más recomendado es realizarlo en términos de 1 año para establecer una frecuencia, de tal manera se puede

establecer una escala de probabilidad de ocurrencia como se muestra en la siguiente tabla:

Tabla 3. Escala de probabilidad de ocurrencia

MA	A	M	B	MB
100	10	1	1/10	1/100
Muy frecuente	Frecuente	Normal	Poco frecuente	Muy poco frecuente
A diario	Mensualmente	Una vez al año	Cada varios años	Siglos

Nota. MAGERIT– versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

3.3. Determinación del impacto potencial

El impacto potencial, se le llama a la medida del daño sobre un activo en particular, a partir de la materialización de una amenaza, este impacto se puede determinar una vez se haya establecido el valor de los activos y la degradación que causa dicha amenaza.

Teniendo en cuenta lo anterior, se establece el impacto de la siguiente manera:

- Se calcula para cada activo, por cada amenaza y en cada dimensión de valoración.

- El impacto se incrementa, cuando mayor es el valor propio de un activo y mayor se degrade el activo de información, así como cuando el activo depende de otros sistemas o viceversa.
- El impacto es mayor de acuerdo con su dependencia del mismo.
- Este impacto, permitirá identificar las consecuencias que tendría una afectación y cómo afectaría a la organización directamente.

El impacto potencial, se puede clasificar de la siguiente manera:

a) **Impacto acumulado:**

- Se tiene como referencia el valor acumulado.
- Las amenazas a las que se puede enfrentar un activo.
- Puede acumularse sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior.
- No se recomienda agregar el impacto acumulado sobre activos que no sean independientes, dado que supondría ponderar el impacto al incluir varias veces el valor acumulado de activos superiores.
- Pueden concluir el impacto de otras amenazas sobre un mismo activo, aunque se recomienda considerar en qué medida las otras amenazas son independientes y pueden ser concurrentes.
- El impacto de una amenaza se puede agregar en diferentes dimensiones.

b) **Impacto repercutido:** se puede aplicar sobre activos de diferente tipo y se determina sobre un activo partir de:

- La importancia para la organización.
- Las amenazas a las que están expuestas los activos de los que depende.
- El impacto de una amenaza se puede agregar en diferentes dimensiones.

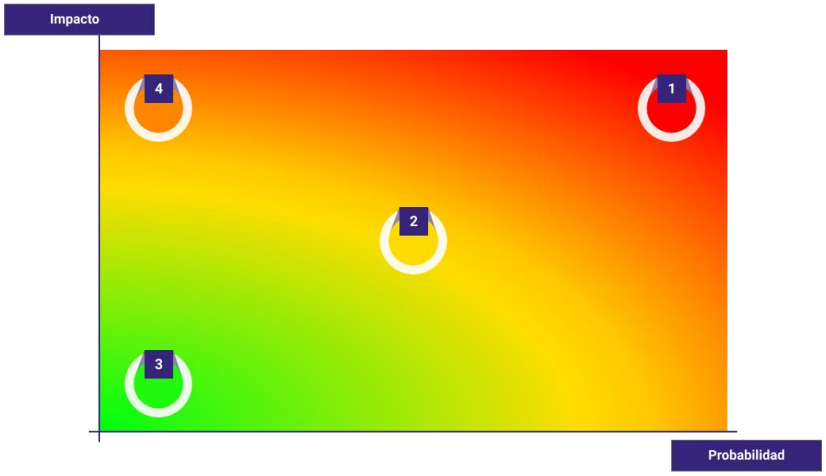
3.4. Determinación del riesgo potencial

El riesgo potencial, se le llama a la medida del daño probable sobre un sistema, teniendo en cuenta el impacto de las amenazas de cada uno de los activos, este riesgo crece con el impacto y la probabilidad, estableciendo las zonas de riesgo como se determinan a continuación:

- **Zona 1:** zona de riesgo muy probable, así como de alto impacto.
- **Zona 2:** franja amarilla: abarca un amplio espectro que representa desde las diferentes situaciones. improbables y de impacto medio, hasta situaciones muy probables, pero de impacto reducido.
- **Zona 3:** riesgos poco probables y de bajo impacto.
- **Zona 4:** riesgos improbables, de muy alto impacto.

Estas zonas se pueden representar en un mapa de calor, como se muestra en la siguiente figura.

Figura 23. El riesgo en función del impacto y la probabilidad



Nota. Recuperado de MAGERIT– versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Se presenta el riesgo en función del impacto y la probabilidad, donde el eje X es la probabilidad y el eje Y corresponde al impacto, mostrando los 4 principales puntos de relación.

A continuación, se va a ampliar la información sobre la clasificación de los riesgos:

Riesgo acumulado

Este riesgo se debe calcular en cada activo amenaza y dimensión de seguridad, convirtiéndose en una función del valor acumulado, la degradación causada y la probabilidad de ocurrencia de la amenaza.

Cuando se calcula sobre los activos base de la información, permite identificar las salvaguardas necesarias para aplicar en los entornos de trabajo: endurecimiento de equipos, “backup”, etc.

Riesgo repercutido

Este riesgo repercutido se obtiene para activo, amenaza y dimensión de valoración, convirtiéndose en una función del valor propio, la degradación causada y la probabilidad de la amenaza.

Este riesgo permite determinar las consecuencias de las incidencias técnicas sobre la finalidad del sistema de información, debido a que se consolida como un recurso gerencial que permite la toma de decisiones críticas de un análisis de riesgos.

Agregación de riesgos: bajo las siguientes condiciones, se permite la agrupación de los riesgos:

- Se puede agregar el riesgo repercutido a diferentes activos.
- Se puede agregar el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común.
- No debe agregarse el riesgo acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el riesgo al incluir varias veces el valor acumulado de activos superiores.
- Puede agregarse el riesgo de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes.
- Se puede agregar el riesgo de una amenaza en diferentes dimensiones.

3.5. Establecimiento de salvaguardas

A partir de este punto se proceden a determinar los controles que serán necesarios para reducir el riesgo y las amenazas; algunas amenazas pueden ser controladas a partir de cambios y acciones de gestión sobre algún activo, pero en otras ocasiones, estas deberán de intervenir a partir de controles técnicos tecnológicos o procedimentales.

A continuación, se describen las acciones que se deben aplicar para reducir el riesgo informático:

Figura 24. Establecimiento de salvaguardas

El establecimiento de salvaguardas está compuesto por:

a. **Selección de salvaguardas**, las cuales son:

- Acciones necesarias para reducir el riesgo sobre un activo.

- Tipo de activos a proteger.
- Dimensión que se requiere mejorar la protección.
- Amenazas sobre las que se actuará.
- Posibles salvaguardas complementarias.

b. **Principios de proporcionalidad**, que consisten en:

- El mayor o menor valor propio o acumulado sobre un activo.
- La mayor o menos probabilidad de que una amenaza se materialice.
- La cobertura que proporciona cada salvaguarda sobre los riesgos.

c. **Tipos de excepciones**, las cuales se dividen en:

- No aplica: cuando una salvaguarda no es adecuada o no se ajusta técnicamente al activo.
- No se justifica: cuando la salvaguarda es adecuada, pero desproporcionada al riesgo que se desea proteger.

d. **Efecto de las salvaguardas**, las cuales son:

- Reducción de la probabilidad de las amenazas.
- Limitación del daño causado.

e. **Declaración de aplicabilidad**, la cual se define como la determinación de las salvaguardas que serán implementadas, cómo se aplicarán, y cuáles no justifican su decisión.

Tipo de protección: la determinación del tipo de protección es fundamental para identificar el tipo de protección, a continuación, en la tabla No. 4 vamos a reconocer los tipos sugeridos por la metodología Magerit.

Tabla 4. Tipos de protección sugeridos por Magerit

Tipo Protección	Descripción
[PR] Prevención	Salvaguardas preventivas que reducen las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos. Ejemplos: autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, metodología segura de desarrollo de "software", pruebas en preproducción, segregación de tareas.
[DR] Disuasión	Salvaguarda disuasoria, tiene efecto sobre los atacantes, reduciendo la intención de que estos se atrevan a atacar un activo. Ejemplos: vallas elevadas, guardias de seguridad, avisos sobre la persecución del delito o persecución del delincuente.
[EL] Eliminación	Son salvaguardas que eliminan un incidente, impidiendo que tenga lugar, lo que significa que actúan antes que el incidente se haya producido. No reducen los daños en caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir. Ejemplos: eliminación de cuentas estándar o sin contraseña y de servicios innecesarios, y en general, todo lo que tenga que ver con la fortificación o bastionado, cifrado de información y armarios ignífugos.
[IM] Minimización del impacto / limitación del impacto	Son salvaguardas que minimizan o limitan el impacto, acotando las consecuencias de un incidente. Ejemplos: desconexión de redes o equipos o detención de servicios en caso de ataque, seguros de cobertura, cumplimiento de la legislación vigente.
[CR] Corrección	Son salvaguardas que actúan después de un incidente, ejerciendo una reparación al activo. Ejemplos: gestión de incidentes, líneas de comunicación alternativas, fuentes de alimentación redundantes.

Tipo Protección	Descripción
[RC] Recuperación	Son salvaguardas que ofrecen recuperación a un activo que ha sufrido una alteración, regresando al estado útil y viable. Ejemplos: copias de seguridad (“back-up”).
[MN] Monitorización	Son salvaguardas enfocadas en la vigilancia y el monitoreo de activos, para identificar posibles cambios o alteraciones en el normal comportamiento de un activo de información. Ejemplos: registros de actividad, registro de descargas de web.
[DC] Detección	Son salvaguardas que detectan un ataque, determinando así lo que está sucediendo. No necesariamente deben detener la acción, pero sí permiten establecer las medidas mínimas necesarias para su protección. Ejemplos: antivirus, IDS, detectores de incendio.
[AW] Concienciación	Son actividades relacionadas con la transferencia del conocimiento para la seguridad de todos los actores involucrados en la organización, y que dependen de los activos de información. Ejemplos: cursos de concienciación, cursos de formación.
[AD] Administración	Son salvaguardas relacionadas con los componentes de seguridad del sistema. Ejemplos: inventario de activos, análisis de riesgos, plan de continuidad.

Nota. Recuperado de MAGERIT– versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

De acuerdo con el modelo anterior, podremos determinar y agrupar las salvaguardas de acuerdo con su efecto sobre una amenaza, como se puede identificar en la tabla No 5.

Tabla 5. Tipos de salvaguardas sugeridos por Magerit

Efecto	A diario
Preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Nota. Recuperado de: https://cutt.ly/DB7caei

Las salvaguardas también por la eficacia en el momento de actuar frente al riesgo para el cual fueron consideradas, una salvaguarda adecuada en 100 % eficaz si combina los siguientes factores:

a) Desde el punto de vista técnico:

- Técnicamente adecuada para enfrentarse al riesgo que protege.
- Aplicación permanente.

b) Desde el punto de vista de operación de la salvaguarda:

- Perfectamente desplegada, configurada y mantenida.

- Existen procedimientos claros de uso normal y en caso de incidencias.
- Los usuarios están formados y concienciados.
- Existen controles que avisan de posibles fallos.

Entre una eficacia del 0 % para aquellas que faltan y el 100 % para aquellas que son idóneas y que están perfectamente implantadas, se estimará un grado de eficacia real en cada caso concreto. Para medir los aspectos organizativos, se puede emplear una escala de madurez que recoja en forma de factor corrector la confianza que merece el proceso de gestión de la salvaguarda:

Figura 25. Eficacia y madurez de las salvaguardas

Factor	Nivel	Significado
0%	L0	Inexistente
	L1	Inicial / "ad hoc"
	L2	Reproducible, pero intuitivo
	L3	Proceso definido
	L4	Gestionado y medible
100%	L5	Optimizado

Nota. Recuperado de: https://cutt.ly/DB7caei

3.6. Impacto residual

De acuerdo con el conjunto de salvaguardas determinadas y desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de

posible impacto que debe ser mínimo, al cual se le denomina residual. Y se consolida una vez hayamos modificado el impacto, desde un valor potencial a un valor residual.

Su cálculo es determinado a partir de la premisa de que un activo no ha sufrido cambio ni degradación, y que las salvaguardas implementadas han actuado de manera positiva evitando la consolidación de algún tipo de incidente.

El impacto residual puede calcularse a partir de los activos inferiores, o repercutido sobre los activos superiores.

Riesgo residual

Este riesgo residual, es calculado a partir del conjunto de salvaguardas implementadas y que conllevan a que un activo no esté sujeto a una potencial alteración en su calidad por ende no ha sido degradado.

El cálculo del riesgo residual se determina de la siguiente manera:

- Tomando como referente que los activos no han cambiado, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.
- La magnitud de la degradación se toma en consideración en el cálculo del impacto residual.
- La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

- El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

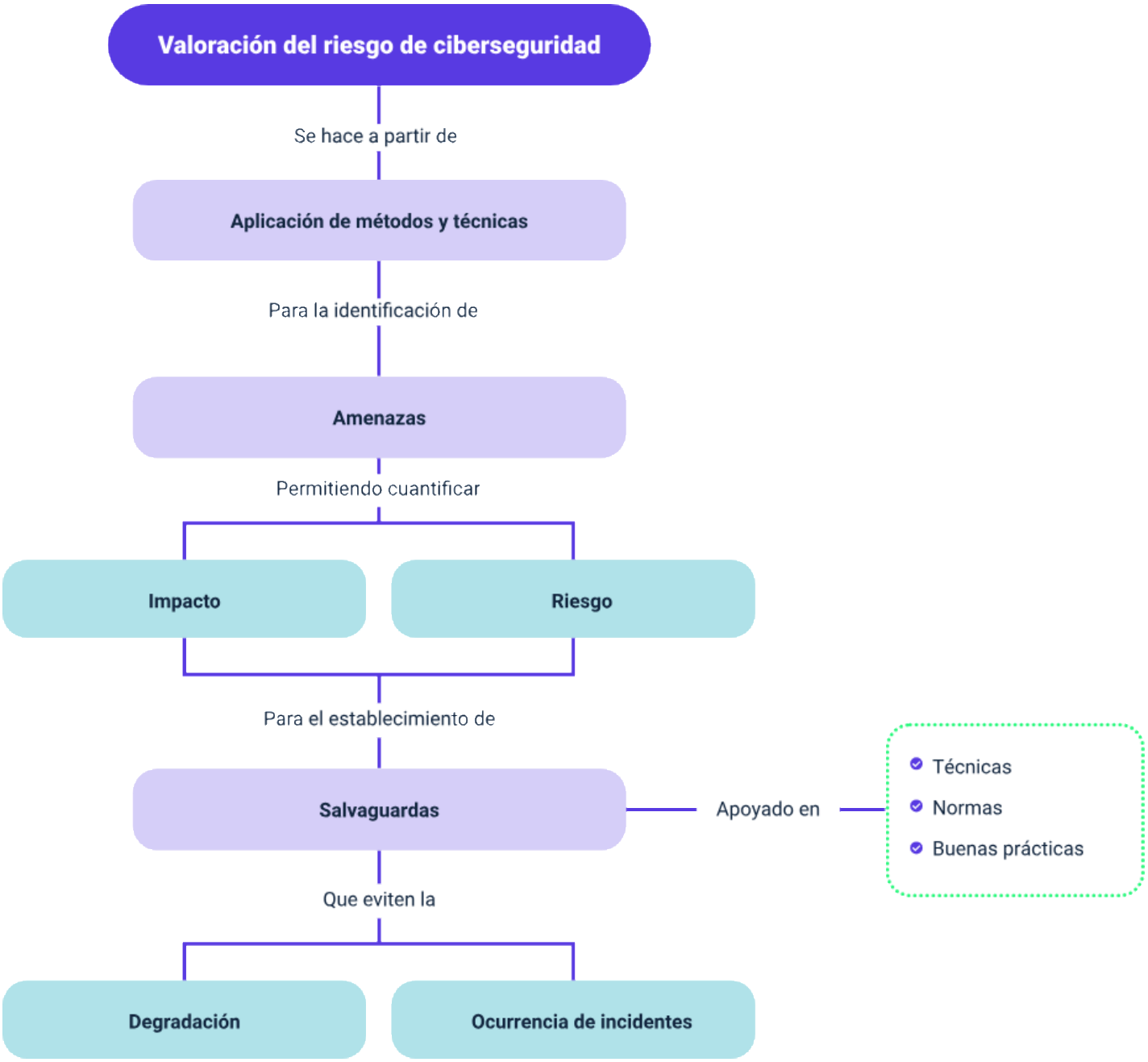
Es así como a partir del establecimiento de las estimaciones y cálculos sugeridos, se permite evaluar y gestionar los riesgos sobre los activos de información en la organización, estos cálculos se pueden implementar en herramientas de gestión o a través de soluciones de hojas de cálculo que permitan realizar un ejercicio práctico y rápido por parte de las organizaciones.

Síntesis

Como hemos podido ver en el presente componente formativo, el ejercicio de evaluación de los riesgos que pueden afectar a los activos en las organizaciones requiere de análisis y valoraciones ajustadas a cada organización en particular, debido a que deben ser evaluados todos los aspectos y particularidades que permiten establecer la importancia y peso de sus activos, así mismo obedece a su sector económico y las condiciones en donde administre información crítica y/o confidencial.

La importancia de adoptar metodologías y técnicas para estos procesos de evaluación del riesgo nos permite mantener una línea estándar para el desarrollo de las actividades y revisión de manera sistémica, así como la revisión periódica para su mejoramiento.

Así mismo, hemos visto cómo la identificación de las salvaguardas adecuadas para la gestión de estos riesgos, tomando como referentes normas internacionales, normas técnicas y buenas prácticas, permite mantener un nivel mínimo aceptable para afrontar los diferentes problemas que presentan las organizaciones.


Valoración del riesgo de ciberseguridad
Se hace a partir de
Aplicación de métodos y técnicas
Para la identificación de
Amenazas
Permitiendo cuantificar
Impacto
Riesgo
Para el establecimiento de
Salvaguardas
Apoyado en
Técnicas
Normas
Buenas prácticas
Que eviten la
Degradación
Ocurrencia de incidentes

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
2. Controles de seguridad	Fernández Rivero, P. P. y Gómez Fernández, L. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. AENOR - Asociación Española de Normalización y Certificación. (p. 36-57).	Libro digital	https://login.bdigital.sena.edu.co/login?qurl=https://elibro.net%2fes%2fereader%2fsenavirtual%2f53624%3fpage%3d36
2. Controles de seguridad	ICONTEC (2018). NTC-ISO 31000:2018 - Gestión del Riesgo. Directrices.	Libro digital	https://e-collection-icontec-org.bdigital.sena.edu.co/normavw.aspx?ID=74790
2. Controles de seguridad	ICONTEC (2018). NTC-ISO-IEC 27001:2013 – Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.	Libro digital	https://e-collection-icontec-org.bdigital.sena.edu.co/normavw.aspx?ID=6387
3. Magerit	PAE, Portal Administración Electrónica. (2012). MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.	Libro digital	https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Glosario

Activo de información: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones ("software"), equipos ("hardware"), comunicaciones, recursos administrativos, recursos físicos y recursos humanos (MAGERIT,2012).

Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Confidencialidad: que la información llegue solamente a las personas autorizadas.

Disponibilidad: disposición de los servicios a ser usados cuando sea necesario.

Integridad: mantenimiento de las características de completitud y corrección de los datos.

PHVA: ciclo determinado por Planear, Hacer, Verificar y Actuar.

Salvaguarda: procedimientos o mecanismos tecnológicos que reducen el riesgo.

Trazabilidad: aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

Vulnerabilidad: toda debilidad que puede ser aprovechada por una amenaza.

Referencias bibliográficas

Escorial Bonet, Á., Escalera Alcázar, J. & Simón Quintana, S. (2019). Guía para la aplicación de UNE-ISO 31000:2018. AENOR - Asociación Española de Normalización y Certificación. https://www.riskia.com/Files/archivos/noticias/9788481439700_extracto.pdf

ICONTEC. (2018). NTC-ISO 31000:2018 - Gestión del Riesgo. Directrices. https://e-collection-icontec-org.bdigital.sena.edu.co/normavw.aspx?ID=74790

INCIBE. (2017). Gestión de riesgos - Una guía de aproximación para el empresario. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

MINTIC. (2016). Seguridad y Privacidad de la Información - Guía de gestión de riesgos. https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Tamayo Saborit, M. & González Capote, D. (2020). La gestión de riesgos: herramienta estratégica de gestión empresarial. Editorial Universo Sur. https://allspace.ucf.edu.cu/index.php/s/cNBoWzkwp32R8A4

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal	Líder del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Hernando José Peña Hidalgo	Experto temático	Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander
Alix Cecilia Chinchilla Rueda	Asesor Metodológico	Centro de Diseño y Metrología - Regional Distrito Capital
Diego E. Acevedo Guevara	Diseñador Instruccional	Centro Industrial del Diseño y la Manufactura - Regional Santander
Sandra Patricia Hoyos Sepúlveda	Correctora de Estilo	Centro de diseño y Metrología - Regional Distrito Capital
Francisco José Lizcano Reyes	Desarrollador Fullstack	Centro Industrial del Diseño y la Manufactura - Regional Santander
Juan Daniel Polanco Muñoz	Diseñador de Contenidos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Wilson Andrés Arenales Cáceres	Storyboard e Ilustración	Centro Industrial del Diseño y la Manufactura - Regional Santander
Carmen Alicia Martínez Torres	Animador y Productor Multimedia	Centro Industrial del Diseño y la Manufactura - Regional Santander
Emilsen Alfonso Bautista	Actividad Didáctica	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruiz Torres	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Regional y Centro de Formación
Luis Gabriel Urueta Álvarez	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniel Ricardo Mutis Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Centro Industrial del Diseño y la Manufactura - Regional Santander