Introducción

Introducción a los riegos de seguridad de la información

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos y de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Teniendo en cuenta que la explotación de un riesgo causaría daños o pérdidas financieras o administrativas a una empresa u organización, es necesario poder estimar la magnitud del impacto del riesgo a que se encuentra expuesta dicha organización mediante la aplicación de controles.

Dichos controles, para que sean efectivos, deben ser implementados en conjunto formando una arquitectura de seguridad con la finalidad de preservar las propiedades de confidencialidad, integridad y disponibilidad de los recursos objetos de riesgo (u otras dimensiones requeridas para la organización como la trazabilidad).

Los riesgos de seguridad de información deben ser considerados en el contexto del negocio, y las interrelaciones con otras funciones de negocios, tales como recursos humanos, desarrollo, producción, operaciones, administración, TI, finanzas, legal, etcétera, y los clientes deben ser identificados para lograr una imagen global y completa de estos riesgos.

Cada organización tiene una misión. En esta era digital, las organizaciones que utilizan sistemas tecnológicos para automatizar sus procesos o información deben de ser conscientes de que la administración del riesgo informático juega un rol crítico para asegurar dicha misión.

La meta principal de la administración del riesgo informático debería ser proteger a la organización y su habilidad de manejar su misión, no solamente la protección de los elementos informáticos. Además, el proceso no solo debe de ser tratado como una función técnica gestionada por los expertos en tecnología que operan y administran los sistemas, sino como una función esencial de administración por parte de toda la organización.

La administración de riesgos es el proceso de identificación, evaluación y toma de decisiones para reducir el riesgo a un nivel aceptable.

El análisis de riesgo informático es un elemento que forma parte del programa de gestión de continuidad de negocio (Business Continuity Management). En este proceso es necesario identificar si existen controles que ayudan a minimizar la probabilidad de ocurrencia de la vulnerabilidad (riesgo controlado), de no existir, la vulnerabilidad será de riesgo no controlado.

Definiciones

Antes de poder continuar, es necesario el poder manejar con soltura determinados términos que aparecerán a lo largo de este curso (basadas en el glosario de MAGERIT v3).

Los términos más importantes y básicos son los siguientes:

- Activo: 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.
- Amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización (fuego, robo de datos, infección por malware, etc).
- Vulnerabilidad: Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. Propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia.
- Impacto: Consecuencia que sobre un activo tiene la materialización de una amenaza (Consecuencia: Resultado de un suceso que afecta a los objetivos).
- Probabilidad (o likelihood) Posibilidad de que un hecho se produzca. En la terminología de la gestión del riesgo, la palabra “probabilidad” se utiliza para indicar la posibilidad de que algún hecho se produzca, que esta posibilidad está definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando

términos generales o de forma matemática (tales como una probabilidad o una frecuencia sobre un periodo de tiempo dado).
- Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. Efecto de la incertidumbre sobre la consecución de los objetivos. Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización. Probabilidad de que una vulnerabilidad propia de un sistema de información sea explotada por las amenazas a dicho sistema, con el objetivo de penetrarlo. De forma menos formal se puede definir como el impacto causado por la combinación de una vulnerabilidad explotada para hacer real una amenaza sobre un activo o conjunto de activos concretos.

A continuación se puede ver la relación entre los mismos (cortesía de la guía de gestión de riesgos del INCIBE):

Otros términos necesarios son los siguientes:

- Análisis de riesgos: Proceso que permite comprender la naturaleza del riesgo y determinar el nivel del mismo. Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (activos) para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.
- Gestión (o tratamiento) del riesgo: Actividades coordinadas para dirigir y controlar una organización el lo relativo al riesgo. Selección e implantación de las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos.

- Informe de estado de riesgo: Caracterización de los activos por su riesgo residual; es decir lo que puede pasar tomando en consideración las salvaguardas desplegadas.
- Informe de evaluación de salvaguardas: Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.
- Impacto residual: Impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información.
- Mapa de riesgos: Informe con la relación de las amenazas a que están expuestos los activos.
- Riesgo acumulado: Dícese del calculado tomando en consideración el valor propio de un activo y el valor de los activos que depende de él. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma.
- Riesgo potencial (o inherente): Riesgos potenciales. Los riesgos del sistema de información en la hipótesis de que no hubieran salvaguardas presentes.
- Riesgo residual: Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información.
- Apetito, Tolerancia y Capacidad del riesgo: El apetito es el nivel de riesgo que la empresa quiere aceptar de acuerdo a sus preferencias (determinadas empresas pueden aceptar un mayor riesgo si puede traer algún tipo de beneficio mientras que otras son más cautelosas), una ponderación de alto nivel de cuánto riesgo la administración y el consejo están dispuestos a aceptar en el logro de sus meta. La tolerancia es el nivel aceptable de variación respecto al apetito en relación a la consecución de un objetivo. Por último, la capacidad es el máximo de riesgo que una organización puede soportar en la persecución de sus objetivos.
- Salvaguarda (Control, medida de seguridad o contramedida): Procedimiento o mecanismo tecnológico que reduce el riesgo. Control o Medida que modifica un riesgo.
- Valor de un activo: Estimación del coste inducido por la materialización de una amenaza.

Gestión del riesgo TI vs Gestión de riesgos para proyectos TI

La gestión de riesgos TI es una aproximación global que busca proteger todos los activos de la organización, especialmente la información, en su procesamiento/tratamiento en los sistemas de información.

Por ello debe ser un proceso continuo que se adapte a los cambios en la organización, tanto en los propios activos como en los riegos potenciales a dichos activos. Esto implica que los análisis de riesgos aportan una imagen estática, una foto, de la organización, en un momento dado. Dado que el entorno es variable en el tiempo (debido a cambios en la información gestionada, las leyes y regulaciones, las posibles amenazas, cambios en los sistemas de información, etc), esta foto debe ser realizada de forma periódica con el objetivo de mantener un conjunto de salvaguardas adecuado y un nivel de riesgo aceptable por la organización (adecuado a su apetito del riesgo).

Por otro lado, tenemos proyectos TI que tienen un comienzo y un final, es decir, definidos en el tiempo, pero que también pueden suponer un riesgo a la seguridad de la información, bien por las tecnologías introducidas (el objetivo de cada proyecto TI) o bien por el propio proyecto en si en caso de no gestionarse adecuadamente (siempre circunscritos al ámbito de la seguridad de la información, dado que existen otros riesgos de proyectos como la existencia de recursos insuficientes o que se extienda un proyecto por encima de lo planificado, y estos riesgos no entran dentro del alcance de este curso y que caerían del lado de metodologías como las del Project Management Institute o del Scrum Institute).

En el caso de los proyectos, se puede aplicar la misma metodología general de análisis y gestión del riesgo TI, teniendo en cuenta sin embargo que, dependiendo de su duración, solo se tendrá una o unas pocas fotos del estado del riesgo en un momento determinado, y que debido a la incertidumbre, la monitorización del riesgo (nivel de riesgo existente, detección de desviaciones, análisis de la efectividad de los controles, etc), deberá ser mucho mayor y más ágil (dado que se trata de un entorno en constante cambio).

Gobierno, Riesgo y Cumplimiento

Gobierno, Riesgo y Cumplimiento (GRC) se refiere a una estrategia para administrar el gobierno general de una organización, la administración de riesgos empresariales y el cumplimiento de las regulaciones. Se trata de un enfoque estructurado para alinear TI con los objetivos de negocio, al tiempo que gestiona eficazmente los riesgos y cumple con los requisitos de cumplimiento.

Una estrategia GRC bien planificada tiene muchos beneficios: mejora de la toma de decisiones, inversiones óptimas en TI, eliminación de silos y reducción de la fragmentación entre las divisiones y departamentos, entre otros.

En el entorno de TI, GRC tiene tres componentes principales:

- Gobierno (o Gobernabilidad): garantizar que las actividades de la organización, como la gestión de las operaciones de TI, estén alineadas de manera que apoyen los objetivos empresariales de la organización.
- Riesgo: asegurarse de que cualquier riesgo (u oportunidad) asociado con las actividades de la organización se identifica y se aborda de una manera que apoya los objetivos de negocio de la organización. En el contexto de TI, esto significa tener un proceso integral de gestión de riesgos de TI que se convierta en la función de gestión de riesgos empresariales de una organización.
- Cumplimiento: asegurarse de que las actividades de la organización funcionen de manera que cumpla con las leyes y reglamentos que afectan a esos sistemas. En el contexto de TI, esto significa asegurarse de que los sistemas informáticos, y los datos contenidos en esos sistemas, se utilizan y se aseguran correctamente.

Las organizaciones desarrollan un marco de GRC para el liderazgo, organización y operación de las áreas de TI de la organización para asegurar que apoyan y permiten los objetivos estratégicos de la organización.

Las funciones de toma de decisiones, gestión de recursos y cartera, gestión de riesgos y cumplimiento normativo incluidas en un marco GRC no serán efectivas a menos que el liderazgo ejecutivo de la organización realmente apoye el cambio cultural, y esto debe incluir a toda la organización y ser desarrollada mediante un proceso “top-down” en la que la gerencia apoye y de recursos de forma clara a dicho proceso, creando una cultura que involucre a todos los estamentos de forma clara (p.e. mediante la definición de objetivos de GRC en todos los niveles).

Gobierno del riesgo vs Gestión del riesgo

El gobierno del riesgo es un framework (marco de trabajo), mientras que la gestión del riesgo es un mecanismo, aunque los dos deben ir de la mano.

Las “reglas del juego” del marco de trabajo del negocio son establecidas por el consejo de dirección, los inversores, la estrategia de negocio, el valor del negocio, la responsabilidad corporativa y el riesgo gestionado, asegurando que los riesgos son identificados, minimizados y controlados dentro del riesgo del apetito de la organización.

El gobierno es un marco de políticas y procesos que permiten al consejo gobernar y reportar a los accionistas y terceras partes. El gobierno se guía primero por la gestión del riesgo como flujos de delegación desde el consejo hacia el resto de la organización. Esto incluye el gobierno de la primera línea de defensa (Operaciones de seguridad), la segunda línea de defensa (Gestión del riesgo) y la tercera (Auditoría, interna y externa), permitiendo a cada una crear valor o proteger contra la pérdida de valor y actuar como facilitadores.

El gobierno y la gestión del riesgo están íntimamente conectados. El primero introduce los artefactos de gobiernos requeridos para la gestión (como las políticas y procedimientos, los procesos, etc), así como otros elementos requeridos como el apetito del riesgo. El segundo identifica, cualifica y evalúa el riesgo para determinar dónde se requiere mayor o menor gobierno. Así mismo, el gobierno actúa como el pegamento que mantiene juntas todas las piezas de la gestión del riesgo. Por ello, a menos que el gobierno del riesgo se estructure adecuadamente, la gestión del riesgo no puede funcionar correctamente. Al revés también es cierto. Si bien el gobierno del riesgo (y de la seguridad en general) puede existir sin la gestión del riesgo, esta le da al gobierno la fortaleza para poder tomar decisiones y avanzar en los procesos de seguridad y la estrategia, a la vez que permite priorizar esfuerzos y recursos. El riesgo es la incertidumbre asociada con la realización de negocios y el gobierno y el cumplimiento son los procesos para proteger al negocio de dicho riesgo.

De forma muy simplificada y condensada, se debe disponer de un gobierno de la seguridad y del riesgo primero, que dará soporte a la gestión del riesgo, mientras que la segunda retroalimentará a la organización con el mapa de riesgos actual de forma que se pueda decidir sobre la mejor estrategia de tratamiento del riesgo en base a las reglas establecidas por el gobierno (priorización, apetito del riesgo, etc).

Por último, destacar también que el gobierno y la gestión del riesgo deben estar alineadas con los objetivos corporativos como los financieros, estratégicos, de reputación, etc con la finalidad se convertirse en un facilitador del negocio en lugar de un centro de coste. El éxito de una organización está en gran parte motivado por cómo de bien toma riesgos y cómo de efectivamente los gestiona.

Definición del marco de gestión del riesgo

Introducción

Con el objeto de poder gestionar el riesgo, primero es necesario contar con un “framework” o marco para el mismo dentro de la organización que define roles y responsabilidades, políticas y procedimientos, recursos, etc. Esto permitirá homogeneizar el proceso y asegurar su repetibilidad en el tiempo así como su completitud y efectividad.

El marco del riesgo establece el contexto y provee de una perspectiva común sobre cómo las organizaciones gestionan el riesgo.

Su principal salida es la estrategia de gestión del riesgo que permite dirigir como las organizaciones pretenden valorar el riesgo, responder a este y monitorizar el mismo. La estrategia de gestión del riesgo hace explícitas las asunciones específicas, las restricciones, la tolerancia al riesgo y las prioridades y contrapartidas utilizadas en la organización para las decisiones de inversión y operacionales.

La estrategia también incluye cualquier decisión a nivel estratégico y las consideraciones sobre cómo los riesgos a las operaciones y activos serán gestionadas por el comité de dirección y la gerencia senior.

Marco de gestión ISO 27005

ISO 27005 es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001.

ISO-27005 es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización. No recomienda una metodología concreta, sino que dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria.

ISO 27005 muestra un enfoque directamente centrado en “Risk Management” para Tecnologías de la Información. Este enfoque tiene que estar alineado con la Gestión de Riesgos Empresarial general de la compañía. Esta norma parte del mismo modelo definido en ISO 31000 (gestión riesgo empresarial general).

Gracias a esta norma se pueden seguir unas pautas para gestionar riesgos en Tecnologías de la Información, tales como aquellos originados por aplicaciones en condiciones vulnerables, sistemas operativos sin actualizaciones o tecnologías obsoletas, por poner unos ejemplos.

De acuerdo a la norma ISO 27005, se establece un contexto en el que se indica un enfoque y criterios de evaluación, impacto y aceptación, se definen alcances y límites y se organiza la Gestión de Riesgos de Seguridad de la Información.

La evaluación de riesgos de Seguridad de la Información comprende la identificación, análisis y evaluación de los riesgos:

- Identificación del riesgo:
  - Introducción.
  - Identificación de activos.
  - Identificación de amenazas.
  - Identificación de controles existentes.
  - Identificación de vulnerabilidades.
- Análisis del riesgo:
  - Metodologías.
  - Evaluación de las consecuencias.
  - Evaluación de la probabilidad de los incidentes.
  - Determinación del riesgo.
- Evaluación de riesgos.

La norma ISO 27005 también comprende el tratamiento de riesgos, la aceptación del riesgo, la comunicación y consulta, el monitoreo y revisión.

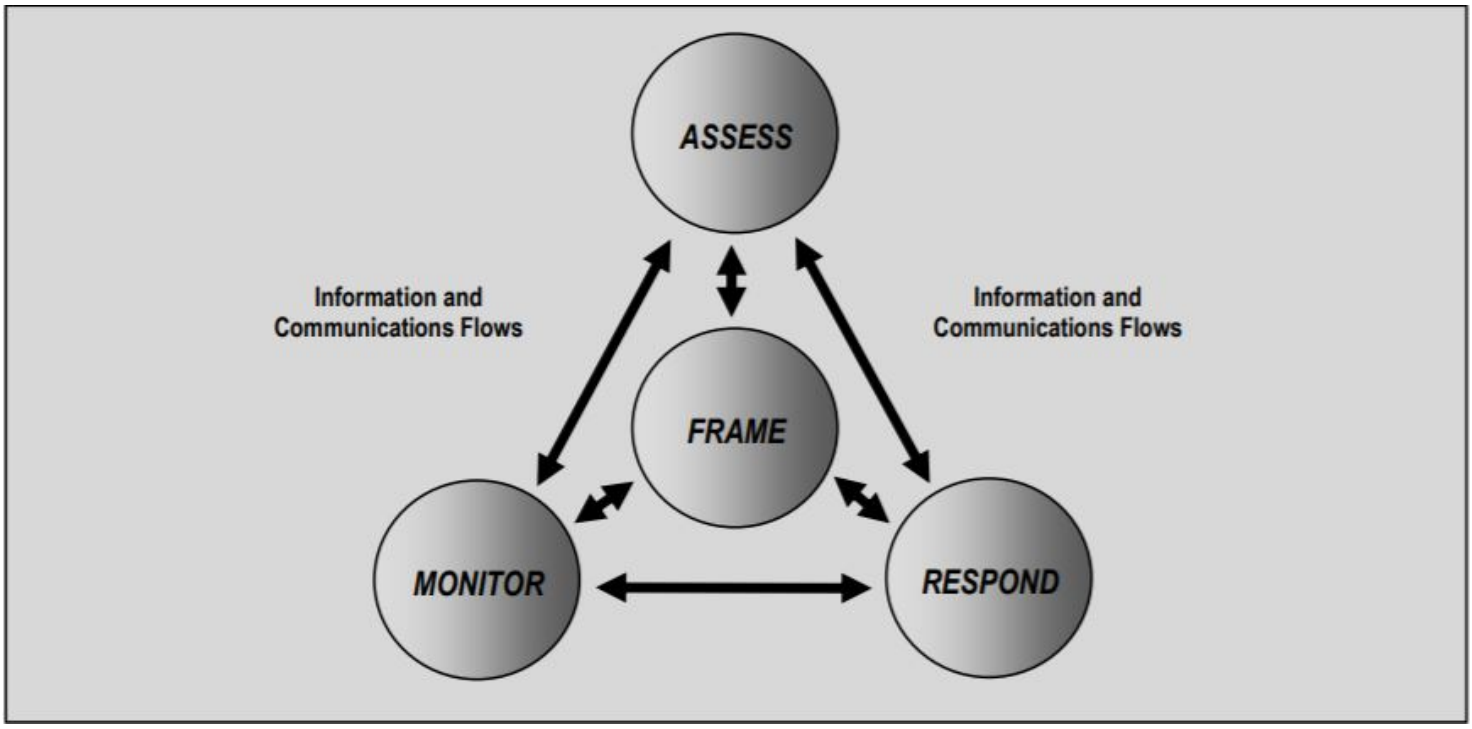
Estándares NIST 800-39 y 800-30

NIST es una organización de EEUU publicando estándares para sus organismos públicos y las organizaciones que trabajan con los mismos, si bien dichos estándares pueden ser utilizados de forma libre en cualquier organización.

El propósito de NIST SP 800-39 es proporcionar una guía para la organización en la gestión de riesgos de seguridad de información. Otro factor importante es proporcionar orientación para desplegar un sistema integrado para toda la organización del programa para la gestión de riesgos de seguridad de información.

La publicación especial 800-39 proporciona un enfoque estructurado, pero flexible para la gestión de riesgos de la información de seguridad que es intencionalmente de base amplia, con los detalles específicos de la evaluación, respuesta y seguimiento del riesgo de forma continua proporcionada por otros que apoyan los estándares del NIST y directrices de seguridad.

A continuación se puede ver el proceso seguido para la gestión integral del riesgo de seguridad de este estándar:



Las flechas negras representan los flujos primarios dentro del proceso de gestión del riesgo, con el marco del riesgo informando a todo el conjunto de actividades secuenciales que van desde la evaluación del riesgo a la respuesta al riesgo y a la monitorización del riesgo.

Por ejemplo, una de las salidas principales del componente del marco del riesgo es la descripción de las fuentes y métodos que la organización utiliza para la adquisición de información de amenazas (p.e. fuentes abiertas, informes de inteligencia clasificados, etc.). La salida concerniente a la información de amenazas es una entrada primaria para el componente de evaluación del riesgo y se debe comunicar a dicho componente.

Otro ejemplo se ilustra en la salida primaria del componente evaluación del riesgo, la determinación del riesgo. Dicha salida es comunicada al componente respuesta al riesgo y recibida como entrada primaria para este componente. Otra entrada primaria para la respuesta al riesgo es una salida del componente marco del riesgo, la estrategia de gestión que define cómo la organización debería responder al riesgo (y aquí podemos ver perfectamente la relación entre gobierno y gestión del riesgo como se definió en un capítulo anterior). Juntas, estas entradas junto con otras adicionales, se utilizan por los decisores para la selección entre los cursos de acción potenciales para las respuestas al riesgo.

La naturaleza bidireccional de las flechas indica que la información y la comunicación fluyen entre los componentes de la gestión del riesgo así como el orden de ejecución de los componentes, que puede ser flexible y responder a la naturaleza dinámica del proceso. Por ejemplo, nueva legislación, directivas o políticas pueden requerir implementar nuevas medidas de respuesta inmediatamente. Esta información se comunica desde el componente de marco del riesgo al de respuesta al riesgo donde las actividades específicas se ejecutan para alcanzar el cumplimiento con la nueva legislación, políticas o directivas.

Si el estándar NIST 800-39 establece un marco y proceso para la gestión del riesgo de sistemas de información en la organización, el estándar NIST 800-30 se centra específicamente en ser una guía para realizar evaluación de riesgo en TI.

Esta publicación se centra en el componente de evaluación del riesgo de la gestión del riesgo integral, proveyendo de un proceso paso a paso para las organizaciones sobre cómo preparar las evaluaciones del riesgo, cómo conducir dichas evaluaciones, cómo comunicar

los resultados al personal clave de la organización y cómo mantener la evaluación del riesgo en el tiempo.

Las evaluaciones de riesgos no son una actividad puntual que provee de información permanente y definitiva a los decisores de la organización para guiar e informar las respuestas a los riesgos de seguridad de la información. Más bien las organizaciones utilizan las evaluaciones del riesgo de forma continua a través del ciclo de vida de desarrollo y de todas las capas de la jerarquía de gestión del riesgo, con la frecuencia de las evaluaciones y los recursos empelados de acuerdo al propósito y alcance específicos definidos explícitamente en la organización.

El segundo componente de la gestión de riesgos se ocupa de cómo las organizaciones evalúan el riesgo en el contexto del "marco de riesgo" de la organización. El objetivo del componente de la evaluación de riesgos es identificar:

- Las amenazas a las organizaciones (es decir, operaciones, activos o individuos).
- Las vulnerabilidades internas y externas a las organizaciones.
- El daño (es decir, el impacto adverso) que puede ocurrir dado el potencial de las amenazas explotando vulnerabilidades.
- La probabilidad de que el daño se producirá. El resultado final es una determinación del riesgo (es decir, por lo general en función del grado de daño y la probabilidad de que se produzcan daños).

Establecimiento del marco de gestión del riesgo

Este modelo de marco de gestión del riesgo se basa en el estándar NIST 800-39.

En el nivel 1 de responsabilidad, los líderes de la organización, con la colaboración del responsable del riesgo deben definir el marco de riesgo organizacional, incluyendo el tipo de decisiones de riesgo soportadas (p.e las respuestas al riesgo), cómo y bajo qué condiciones se evaluará el riesgo para dar soporte a las decisiones sobre el riesgo (de forma regular y cuñando, ante cambios de impacto y cuáles serían estas condiciones, etc) y cómos e monitorizará el riesgo (p.e hasta qué nivel de detalle, de qué forma o con qué frecuencia). En el nivel 2 de responsabilidad, los propietarios de los servicios/procesos (p.e los responsables de cada área funcional y de soporte si fuese necesario) aplicarán su comprensión del marco organizacional del riesgo para dirigir sus preocupaciones específicas a las funciones de negocio (p.e asunciones adicionales, restricciones, prioridades y concesiones). En la capa 3, los responsables de programas, propietarios de SI y los proveedores comunes de controles (p.e el área de ciberseguridad) aplican su entendimiento del marco de riesgo de la organización en base a como los decisores en las capas 1 y 2 decidieron gestionar el riesgo. El marco de gestión del riesgo es el medio principal para dirigir el riesgo en la capa 3. El marco trata preocupaciones sobre el diseño, desarrollo, implementación, operación y eliminación de los SI organizacionales y los entornos en los que estos operan.

En caso de que no existiese este marco, la capa 2 podría tener perspectivas divergentes sobre el riesgo o cómo gestionarlo. Esto impediría una comprensión común en la capa 1 sobre cómo la seguridad de la información contribuye al riesgo organizacional, y en la capa 2 sobre cómo el riesgo aceptado para un área/servicio/proceso afecta a otras áreas/servicios/procesos. Las diferencias en la tolerancia al riesgo y las asunciones subyacentes, restricciones, prioridades y concesiones están sustentadas en consideraciones arquitectónicas u operacionales y deberían ser entendidas y aceptadas por la capa 1.

El trabajo previo para crear este marco estandarizado para la organización será el siguiente:

- Identificar las asunciones que afectan a cómo el riesgo se evalúa, se responde y se monitoriza en la organización: Las organizaciones que identifican, caracterizan y proveen ejemplos representativos de las fuentes de amenazas, vulnerabilidades, consecuencias/impacto y determinaciones de probabilidades promocionan una terminología común y un marco de referencia para comparar y tratar el riesgo a través de diferentes áreas / servicios / procesos. Las organizaciones también pueden seleccionar las metodologías apropiadas de evaluación del riesgo dependiendo del gobierno establecido, la cultura y cómo de diferentes son las áreas/servicios/procesos. Por ejemplo, es organizaciones con estructuras de gobierno altamente centralizadas se podría seleccionar una metodología común para toda la organización, mientras que organizaciones con estructuras de gobierno híbridas podrían seleccionar diferentes metodologías para la capa 2 y una metodología de evaluación del riesgo adicional para la capa 1 que asimile y armonice los resultados de las evaluaciones en la capa 2.
- Identificar restricciones para la realización de las actividades de evaluación, respuesta y monitorización del riesgo dentro de la organización: La ejecución del proceso de gestión del riesgo puede ser constreñida de varias formas, algunas directas y otras indirectas.
    - Las limitaciones financieras pueden constreñir el conjunto de actividades de forma directa (p.e limitando los recursos totales asignados para invertir en la gestión del riesgo, como en evaluaciones o en salvaguardas) o indirecta (p.e eliminando actividades que, si bien entrañan inversiones relativamente pequeñas en respuesta a los riesgos, suponen la reducción o el descarte de inversiones en sistemas de información o tecnología de la información heredados o "lagacy"). Las organizaciones también pueden descubrir la necesidad de continuar dependiendo de sistemas heredados que podrían limitar las opciones de gestión del riesgo disponibles.
    - Las restricciones también pueden incluir requisitos legales, regulatorios y/o contractuales. Tales restricciones pueden reflejarse en las políticas de la organización (p.e restricciones en la contratación, restricciones y/o requisitos para la información que debe ser recogida para la monitorización del riesgo, etc).
    - La cultura organizacional puede imponer restricciones indirectas en cambios del gobierno (p.e impedir el paso de estructuras de gobierno descentralizadas a híbridas) y qué controles de seguridad son considerados por las organizaciones

como controles comunes.
- Identificar el nivel de tolerancia al riesgo de la organización: La tolerancia al riesgo es el nivel de riesgo que una organización está dispuesta a a aceptar en su búsqueda de objetivos estratégicos. Las organizaciones definen la tolerancia al riesgo de seguridad de la información a nivel organizacional considerando todas las áreas / servicios / procesos. Se pueden utilizar diversas técnicas para identificar el nivel de tolerancia (p.e estableciendo zonas en un espacio comercial de impacto probable o utilizando un conjunto de escenarios representativos).
- Identificar las prioridades y compensaciones consideradas por la organización para la gestión del riesgo: El riesgo se experimenta en diferentes niveles, en diferentes formas y en diferentes tiempos. En la capa 1, las organizaciones realizan concesiones y establecen prioridades para responder a esos riesgos. Las organizaciones tienden a tener múltiples prioridades que a veces entran en conflicto, lo que genera un riesgo potencial. Los enfoques empleados por las organizaciones para la gestión de las carteras de riesgos reflejan la cultura de la organización, la tolerancia al riesgo, así como las hipótesis y limitaciones relacionadas con el riesgo. Estos enfoques suelen estar incorporados en los planes estratégicos, las políticas y las hojas de ruta de las organizaciones, que pueden indicar las preferencias por diferentes formas de respuesta al riesgo. Por ejemplo, las organizaciones pueden estar dispuestas a aceptar el riesgo a corto plazo de operaciones ligeramente degradadas para lograr la reducción a largo plazo del riesgo de seguridad de la información. Sin embargo, esta compensación podría ser inaceptable para una función comercial particularmente crítica (por ejemplo, las necesidades en tiempo real de muchos sistemas de control industrial o de procesos). Para esa esfera de alta prioridad, tal vez sea necesario adoptar un enfoque diferente para mejorar la seguridad, incluida la aplicación de controles de seguridad compensatorios.

De todas formas, en muchas organizaciones pequeñas/medianas y/o con poco nivel de madurez respecto a la gestión del riesgo, el marco puede establecerse con una línea base básica y seguir madurando a partir de ahí:

- Metodología de análisis de riesgos, incluyendo valores posibles para la probabilidad e impacto (de forma cualitativa; más adelante se entrará en detalle en este modelo de evaluación).
- Catálogo de activos y amenazas.
- Catálogo de potenciales salvaguardas.
- Tolerancia al riesgo simplificada.

Para los catálogos, existen diferentes estándares y metodologías como MAGERIT V3 que pueden ser utilizadas como base y adaptadas a la organización.

Alineación con el negocio

La gestión de riesgos ayuda a mitigar el aumento de amenazas para las organizaciones. El cambio hacia un enfoque de gestión de riesgos de seguridad se ha estado desarrollando por algún tiempo, según el Estudio CISO Insights. Los líderes en seguridad están notando que simplemente marcar casillas para abordar los requisitos de seguridad ya no es una estrategia suficiente. Estos líderes que incrementan la curva de madurez están transformando sus programas para que se basen en verdad en riesgos al utilizar un enfoque sofisticado para determinar riesgos y priorizar las inversiones en seguridad.

A continuación, se mostrarán más requisitos claves que deben poseer los programas gestión de riesgos de seguridad:

- El cumplimiento es solo un factor: El cumplimiento no debe desaparecer en su totalidad incluso en un programa basado en riesgos. Las normas están ahí, pero los jefes y gerentes de un departamento deben empezar a pensar en términos de niveles de riesgo aceptables frente a requisitos de cumplimiento. Este es un cambio en el lenguaje y es el momento cuando todos entienden que la diferencia es la transformación de toda la empresa.
- La tolerancia al riesgo evoluciona con el tiempo: Se espera que un plan de evaluación y un perfil de riesgo cambien con el tiempo. Además, es difícil para las empresas evaluar de manera adecuada el riesgo antes de encontrar un problema. Sin embargo, las conversaciones frecuentes sobre con qué están cómodos los gerentes senior y los jefes promueven la conciencia de riesgos en todas las líneas del negocio.
- Hacer funcionar la gestión de riesgos: La gestión de riesgos se divide en tres áreas distintas: estratégica, táctica y operativa. A medida que una empresa se traslada hacia un enfoque basado en riesgos, puede explorar plataformas de evaluación, trabajar para crear perfiles de riesgo y asociarse con proveedores para realizar una evaluación de riesgos.

Así mismo, para asegurar la madurez del proceso, este debe quedar alineado con el negocio. Se debe pasar de un modelo de centro de costes a uno de facilitador del negocio.

Por ello, en el proceso de identificación del riesgo, es necesario que se consulte a los principales líderes de la organización con el objeto de saber qué activos son especialmente importantes para ellos, qué procesos de transformación sufrirá en el corto y medio plazo la organización, cuáles son los escenarios de amenaza/riesgo que les preocupan de verdad, etc. Con este conocimiento será más fácil adaptar la identificación de activos y amenazas y alinearse con el negocio (a través del pensamiento e inquietudes de los gerentes).

Así mismo, este trabajo debe ser bidireccional, de forma que se facilite a la gerencia, y especialmente al consejo de dirección, el entendimiento de los riesgos de la organización y cómo los mismos pueden afectar a los objetivos del negocio, de forma que se

puedan tomar decisiones razonadas y acordadas entre todas las partes sobre los controles a desplegar y el funcionamiento de los mismos, todos en base a las amenazas existentes en cada momento.

Cultura del riesgo

Una sólida cultura de riesgo es la clave para alinear todos los frentes de una compañía según sus objetivos estratégicos.

En el mundo empresarial, los cambios suceden de manera vertiginosa. Esos movimientos dinámicos e impredecibles producen consecuencias repentinas e inesperadas. Efectivamente, un riesgo puede aparecer en uno de esos instantes y generar diferentes niveles de impacto, combinándose con otros y generando mayores amenazas.

Cuando se filtran los datos de los clientes de un banco, por ejemplo, no solo se incurre en un riesgo de privacidad, sino también en un riesgo reputacional. Incluso, dependiendo del curso de los eventos, se podrían desencadenar en poco tiempo nuevos riesgos, ya sean legales o financieros.

Por eso, es necesario tener una cultura de riesgo que permita reportar, escalar e intervenir los posibles daños o aprovechar las oportunidades. Por supuesto, un riesgo no solo implica un peligro. También puede proporcionar una oportunidad para optimizar áreas vulnerables y mejorar los frentes o las iniciativas de la compañía.

La definición de cultura de riesgo abarca los valores, las creencias, las actitudes y el conocimiento sobre el riesgo que se tiene en el interior de una organización.

Para que sea efectiva debe comenzar por un apropiado ambiente interno de control. En este sentido, es necesario establecer una filosofía de administración, determinar cuál es el nivel de apetito al riesgo, especificar los valores que orientan las operaciones, tener una estructura organizacional clara y unas buenas prácticas para contratar y capacitar al recurso humano.

Luego debe definirse qué sentido tiene la cultura de riesgo dentro de la organización, teniendo en cuenta el propósito, la misión y los valores de la empresa. Esto le permitirá determinar el alcance de la cultura de riesgo de manera explícita. De esa forma será más fácil de difundir y comunicar la cultura de riesgo dentro de todos los niveles de la compañía.

Es importante que esta cultura del riesgo de ciberseguridad sea embebida dentro de la cultura de riesgo general de la organización, dado que es parte de este riesgo global (seguridad, económico, operaciones, etc). De acuerdo con Price Waterhouse Coopers, existen tres líneas de defensa: la primera está conformada por la alta gerencia y las unidades de negocio, la segunda por los comités de riesgo, que es el CRO y la tercera por la auditoría interna.
Aunque el director de riesgo se encuentra en la segunda línea tiene la obligación de interactuar con la primera y la tercera.

Una cultura de riesgos también involucra los cibernéticos, aquí es necesario definir líneas de acción específica en tres áreas: la primera es el uso de una metodología alineada con la estrategia de operación, la segunda son planes flexibles y la tercera consiste en tener una línea de comunicación con los grupos. Cada una de las líneas de gestión de riesgos debe estar alineada con los valores, metas y objetivos de la compañía, de esta forma será más fácil que los colaboradores estén preparados ante cualquier posible problema al que se enfrente la organización.

Roles y responsabilidades

Dependiendo de la organización, los roles y responsabilidades expresados a continuación podrían variar, aunando algunas personas varios roles o bien estando las responsabilidades de algunos roles diluidas en otros. Sin embargo, esto puede servir como una línea base con la que comprar una organización y asegurar que todas las responsabilidades han sido asignadas, independientemente del rol:

- Comité de dirección: El comitñe de dirección es el responsable último de la gestión de riesgos. Si bien delega en la gerencia general su implementación adecuada y eficiente, el directorio tiene la responsabilidad final de la gestión de riesgos, y por lo tanto, debe determinar la estrategia general de gestión de riesgos de la entidad (como el gobierno, establecimiento de una cultura adecuada, la asignación de recursos, etc).
- Comité de riesgos: El comité de dirección debe conformar un comité de riesgos, el cual se reúna periódicamente y que represente a todas las áreas requeridas (legal, operaciones, financiero, ciberseguridad, TI, etc). Además, el comité podrá contar con la participación permanente de asesores externos y del responsable del área especializada en la gestión de riesgos, los cuales podrían tener sólo derecho a voz, pudiendo ser excluidos de las deliberaciones en cualquier momento a petición de un director (dependiendo de la organización y su cultura de toma de decisiones). Todas las decisiones y aspectos relevantes que se traten en el comité deben quedar registrados de manera formal a través de un acta, donde quede constancia de los argumentos entregados por cada uno de los participantes respecto de las materias tratadas en cada sesión, así como los acuerdos alcanzados. Las funciones del comité de riesgos deben comprender al menos:
    - Definir y proponer al comité de dirección, la estrategia y las políticas de gestión de riesgos para la organización.
    - Conocer en detalle los niveles de exposición y los riesgos asumidos con base en la metodología aprobada por el comité.
    - Proponer al comité los criterios de aceptación de los riesgos que se desean gestionar, de acuerdo con su ámbito de actividad, a los objetivos estratégicos y a la metodología de gestión de riesgos establecida y aprobada.

    - Informar al comité de los resultados obtenidos por las diferentes gerencias responsables, en relación a los riesgos asumidos, considerando los informes de gestión y monitoreo de riesgos generados por el área especializada en la gestión de riesgos.
    - Evaluar regularmente la efectividad general de las técnicas de administración e infraestructura tecnológica, para la gestión de riesgos, teniendo como base los informes presentados por el área especializada en la gestión de riesgos, por la unidad de auditoría interna y por los auditores externos.
    - Aprobar los planes de capacitación propuestos por el área especializada en la gestión de riesgos, destinados a fortalecer los conocimientos en materia de riesgos en la organización.
    - Asegurar que los criterios establecidos en las políticas de gestión de riesgos se consideren en la definición de nuevos proyectos y servicios.
- Gerencia general: La gerencia general tiene como responsabilidad ejecutar de forma efectiva y eficiente el modelo de gestión de riesgos, todo ello dentro de las políticas, los manuales y los procedimientos previamente establecidos.
- Áreas funcionales y de apoyo: Las distintas áreas de la organización deben involucrarse activamente en la gestión de los riesgos, siendo responsables del funcionamiento del sistema de gestión de riesgos dentro de su área. Para tal efecto deben contar con el asesoramiento del área especializada en la gestión de riesgos.
- Área especializada en la gestión de riesgos: Las organizaciones deben contar con un área especializada en la gestión de riesgos (generalmente dentro del área de seguridad de la información), la cual debe ser independiente de las áreas funcionales y de apoyo. El comité debería asegurar que el área especializada en la gestión de riesgos, cuente con recursos suficientes para el pleno desarrollo de sus actividades, así como la independencia suficiente para la toma de decisiones. Dicha área debe cumplir, entre otras funciones, con las siguientes:
    - Proveer el marco de políticas para establecer los estándares mínimos de control interno dentro de los cuales la organización debe administrar sus riesgos.
    - Desarrollar, actualizar, proponer cambios y comunicar las estrategias, políticas, manuales, procedimientos y metodología de gestión de riesgos.
    - Dar soporte técnico al comité de dirección y a las demás áreas funcionales y de apoyo, en las distintas actividades necesarias para la implementación y ejecución de la metodología de gestión de riesgos.
    - Conocer en detalle los niveles de exposición y los riesgos asumidos y validados por las distintas áreas funcionales y de apoyo, aplicando procesos de evaluación del riesgo periódicos o cuando cambios importantes en los procesos/servicios lo requieran.
    - Mantener actualizada la información contenida en el registro de riesgos, y apoyar en el reporte de los eventos registrados por las áreas funcionales y de apoyo.
    - Monitorear y evaluar el impacto de los cambios en las normativas, regulaciones, leyes, procesos, y desarrollos de nuevos servicios que alteren el actual mapa de riesgos de la organización.
    - Solicitar, consolidar y monitorear permanentemente los indicadores definidos para los distintos riesgos establecidos en las políticas de gestión de riesgos, así como también los informes sobre la gestión de riesgos.
    - Identificar las necesidades de capacitación y difusión que permitan una mejor gestión de riesgos.
    - Informar de forma regular al comité, al comité de riesgos, al comité de auditoría si corresponde, a la gerencia general y a los dueños de procesos y servicios, sobre el cumplimiento de las políticas y los manuales de gestión de riesgos definidos por la organización, así como también respecto a los indicadores de riesgo definidos y los incidentes más significativos ocurridos.
- Auditoría interna: La unidad de auditoría interna, con dependencia directa del comité, debe evaluar el cumplimiento de los procedimientos utilizados para la gestión de cada uno de los riesgos a los que se ve expuesta la organización, de acuerdo a las exigencias contenidas en las presentes instrucciones. El rol de auditoría interna debe ser independiente del área encargada de la gestión de riesgos, debiendo para ello contar con los recursos necesarios, la independencia y la objetividad, permitiendo con ello entregar información relevante en la toma de decisiones al comité, sobre la calidad de la gestión de riesgos que se realiza en la mutualidad.

Registro del riesgo

El registro del riesgo es un documento o herramienta donde se registran todos los nuevos riesgos que afecten a la organización, de forma que en todo momento se pueda saber el estado de riesgo de la mismo.

Este registro debería ser actualizado de forma regular, tras cada evaluación del riesgos, con cada reunión del comité del comité de riesgos, con los resultados del monitoreo del riesgo y su tratamiento, etc.

Este registro deberá ser un proceso en curso de forma continua, puesto que debe permitir no solo conocer el estado del riesgo en cada momento, sino el estado de los proyectos y operaciones de tratamiento del riesgo, pudiendo detectar desviaciones así como incluir nuevos riesgos ante cambios en la organización o los riesgos (nuevos riesgos o cambios en los existentes; generalmente no se dispone de toda la información sobre cada riesgo al inicio, por lo que podrá varia según se vaya recopilando nueva información, ya sea desde la experiencia en la propia organización o mediante información externa como informes de ciber-inteligencia).

Como mínimo, por cada riesgos e debería recopilar la siguiente información:

- Identificador único.

- Fecha de detección: Cuándo se detectó el riesgo.
- Descripción del mismo.
- Probabilidad.
- Impacto.
- Nivel de riesgo (Probabilidad x Impacto).
- Propietario: Quién es el responsable por su gestión.
- Acciones/Salvaguardas de tratamiento: Qué salvaguardas existen o serán implementadas (con detalle de fechas) para tratar el riesgo y prevenirlo (o bien evitarlo o transferirlo).
- Acción de contingencia: Qué se deberá hacer en caso de que un riesgo se materialice.
- Progreso de las acciones: Actualización regular sobre el estado de las salvaguardas y de la implementación (en los casos donde aún estén en proceso).
- Estado: Abierto, cerrado, En espera, etc.

Evaluación del riesgo

Introducción

El análisis del riesgo ayuda a las personas encargadas de tomar decisiones y a los directivos a entender la gestión de riesgos y cómo pueden afectar a la consecución de sus objetivos, y a la capacidad de eficiencia de los controles ya implantados.

Los resultados de este análisis, nos servirán de referencia a la hora de tomar decisiones en la empresa.

Es la parte del proceso de gestión de riesgos en la que conocemos e inspeccionamos los riesgos.

El objetivo de la identificación del riesgo es conocer los sucesos que se pueden producir en la organización y las consecuencias que puedan tener sobre los objetivos de la empresa.

El procedimiento para la gestión de riesgos contiene el reconocimiento de las causas y la procedencia del riesgo que puedan afectar a los objetivos.

Los procedimientos de identificación del riesgo pueden contener:

- Procedimientos en base a evidencias, como por ejemplo las revisiones de datos anteriores.
- Los enfoques metodológicos del equipo, en el que los expertos identifican los riesgos a través de una serie de preguntas.
- Métodos de razonamiento inductivo, como por ejemplo HAZOP. Un razonamiento inductivo es una forma de razonamiento en que la verdad de las premisas apoyan la conclusión, pero no la garantizan (Todos los cuervos observados hasta ahora son negros / Por ello todos los cuervos son negros).

En esta primera fase de la metodología se identifican de forma sistemática las posibles causas concretas de los riesgos empresariales (de seguridad), así como los diversos y posibles efectos que debe afrontar la organización.

Una correcta identificación y valoración de riesgos requiere un conocimiento detallado de la organización, del mercado en el que opera, del entorno legal que le rodea, lo activos existentes, la relación de interdependencia entre los mismos, etc.

La identificación del riesgo debe ser sistemática y empezar por identificar los objetivos clave de éxito y amenazas que puedan perturbar el logro de dichos objetivos.

Para facilitar la aplicación de los conceptos que se verán en este capítulo, se ofrece a continuación un enlace al proyecto final de carrera de una alumna de ingeniería informática que realizó un ejemplo completo basado en la metodología MAGERIT V3 sobre una empresa real. Este ejemplo, junto con ejemplos más pequeños presentados en este capítulo facilitará obtener una visión práctica de la evaluación del riesgo, así como sobre la metodología MAGERIT en general. Se recomienda ver dicho documento de forma gradual tras obtener el conocimiento teórico para analizar su aplicación en la práctica.

Métodos y herramientas para el análisis del riesgo

Con el objeto de asegurar una recolección de riesgos completa y coherente, se pueden utilizar una serie de herramientas y métodos que facilitarán el análisis de la organización.

Entre las más comunes podemos encontrar:

- Check-lists: Se trata de una manera simple de identificar los riesgos. Esta técnica proporciona una lista de las incertidumbres típicas a considerar. Los usuarios se refieren a una lista previamente desarrollada, códigos o normas (por ejemplo, el catálogo de amenazas de MAGERIT).
- Entrevistas: Se realizan entrevistas con expertos de la organización y/o externos para la dientificaciónd e los riesgos.
- Análisis Delphi: Los responsables de lograr la ejecución del método Delphi, son varios grupos de expertos dotados de un conocimiento amplio en el tema de gestión de riesgos. Para que esta técnica funcione correctamente se deben lograr opiniones anónimas, individuales y en conjunto, con los miembros encargados (de forma que nadie influencie a otros, y sobre todo evitar que una opinión de una persona de alto rango pueda afectar a otros de menor rango). Hay que tener en cuenta que este método no utiliza datos históricos que lo relacionen con estudios anteriormente hechos, por lo que se debe cuidar y supervisar la retroalimentación para lograr que los resultados se generen controladamente. Para lograr la efectividad de esta técnica de evaluación se necesita un proceso adecuado para la identificación de riesgos:
  - Escoger el grupo o los grupos de expertos en el tema a tratar.
  - Formación del equipo encargado de la ejecución de la técnica.
  - Formación de otro grupo encargado de la supervisión del método.
  - Desarrollar un cuestionario.
  - Repartir el primer cuestionario entre los miembros del grupo.
  - La información obtenida del primer cuestionario es recopilada, analizada y discutida.
  - Se realiza un segundo cuestionario combinando las respuestas y buscando un consenso hasta llegar al equilibrio.
- Informes de inteligencia externos: A nivel externo a la organización existen diferentes empresas privadas y organismos públicos que producen informes de inteligencia sobre nuevas amenazas y tendencias, ya sea a nivel general o sectorial. Estos informes pueden ser analizados para ver su posible ocurrencia en la organización. Por un lado se dispone de feeds de ciberinteligencia que alertan de nuevo malware, vulnerabilidades y ataques, junto con posibles indicadores de compromiso (IoCs) para su detección automática mediante herramientas (como un SIEM o un EDR). Por otro, existen organizaciones llamadas ISACs (Information Sharing and Analysis Centers) que proveen de recursos centralizados para la recopilación de información sobre amenazas y que permiten una comunicación bidireccional con sus miembros (de forma que se retroalimenten entre ellos), ofreciendo información sobre experiencias en diferentes causas raíz, incidentes y amenazas, así como la compartición de experiencias, conocimiento y análisis realizados.
- What if: El análisis what if (¿qué pasaría si…?) se usa en la etapa preliminar de la gestión cuando se comienzan a identificar los riesgos. Este método consiste en programar reuniones con expertos que conozcan en detalle un área / servicio / proceso concreto. En la reunión inicial se plantean interrogantes para evidenciar riesgos futuros. Las reuniones siguientes son para encontrar causas, consecuencias y acciones. Se basa en imaginas casos que impactarían en la organización y validar su probabilidad e impacto final.

Así mismo, existen otra serie de técnicas más avanzadas que pueden utilizarse, si bien requieren de un mayor conocimiento así como de una mayor madurez en la organización:

- Análisis preliminar de riesgos (APR): Esta metodología de gestión de riesgos sirve para identificar posibles riesgos al inicio de un proyecto. Como es un análisis sistémico, se aborda cada fase de un proceso específico. Al dividirlo en sus partes, se pueden asociar los riesgos generales a las etapas particulares.
- Cinco porqués: El propósito de este método para gestionar el riesgo es reconocer la causa raíz de un problema. Por medio de preguntas repetitivas, se identifican los orígenes de un evento de riesgo. Esta metodología de riesgos consiste en un trabajo grupal en el que se presenta el problema y se plantean preguntas que lleven a descifrar su causa raíz. El número de preguntas que se haga dependerá de la complejidad del evento que se está analizando.

- FME (Failure mode and effective analysis): El método FMEA busca identificar, clasificar y eliminar anticipadamente los problemas de los proyectos y de los procesos de una empresa. Este método para gestionar el riesgo comienza con la identificación de los errores. Luego estos se clasifican puntuando los riesgos según la frecuencia, la gravedad y la detección. Después de haberlos clasificado y priorizado, se establecen los problemas más graves, que se atienden de manera prioritaria.
- Matriz SWOT (Strenghts, Waknesses, Opportunities and Threats): La matriz SWOT es uno de los métodos principales que debe conocer para gestionar el riesgo. SWOT consiste en el análisis de fortalezas, debilidades, oportunidades y amenazas. Este método comienza con un análisis interno, en el que se identifican las fortalezas y los puntos débiles del negocio. Luego se analiza el contexto externo para identificar oportunidades y amenazas.
- Análisis de árbol de fallas: Esta técnica se inicia con un evento no deseado y determina todas las maneras en las que podría ocurrir. Estos eventos se muestran gráficamente en un diagrama de árbol lógico. Una vez que el árbol de fallas se ha desarrollado, debe considerarse la posibilidad de formas de reducir o eliminar las posibles causas/fuentes, etc.
- Diagrama causa-efecto (o de Ishikawa). Un efecto puede tener un número de factores que se pueden agrupar en distintas categorías. Estos factores se identifican a menudo a través del intercambio de ideas y se muestran en una estructura de “espina de pescado”. Permite conocer la raíz del problema y cuellos de botella en procesos.
- Cuestionario de análisis de riesgos: El cuestionario consiste elaborar una serie de preguntas para definir la probabilidad de que sucedan eventos de impacto. Cada uno de los interrogantes tocan cuestiones que pueden implicar algún riesgo. Después de haber armado la lista, esta debe revisarse y complementarse de acuerdo con los requerimientos de cada proyecto o proceso.
- Gráfica de flujo de procesos: Esta herramienta para analizar el riesgo muestra gráficamente la secuencia de funcionamiento de un proceso, lo cual es importante para determinar el flujo de las actividades de una empresa. En la elaboración de estos diagramas, se utiliza nomenclatura estandarizada por organizaciones como la ISO y la ANSI, lo que facilita su comprensión sin importar el proceso que se esté describiendo. Así, se podrán detectar potenciales problemas y amenazas en dichos pasos que afectarían al proceso.
- Análisis Modal de Fallos y Efectos (AMFE): Esta técnica identifica y analiza los fallos potenciales, mecanismos y los efectos de esos fallos. Entre otros, se utiliza para el diseño de componentes y productos, sistemas, procesos de fabricación y montaje, servicio y software.
- Análisis funcional de operatividad (HAZOP). Se trata de un proceso general de identificación de riesgos para definir posibles desviaciones del rendimiento esperado o deseado. Se utiliza para detectar situaciones de inseguridad en plantas industriales, debido a la operación o a los procesos productivos.
- Análisis de capas de protección (LOPA). Permite la evaluación de controles, así como su eficacia.
- Análisis de Montecarlo: El análisis de Montecarlo es un método utilizado para, mediante una simulación matemática compleja, aproximar el resultado de cálculos de los que no se puede obtener una solución exacta. Es un método que se utiliza para realizar estimaciones en caso de que existan parámetros que muestran variabilidad. Así, se general multitud de simulaciones con diferentes variaciones en las variables de forma aleatoria (mediante el uso de ordenadores) de forma que se pueda obtener una representación de los valores más probables.

Se puede encontrar más información sobre estas técnicas en el libro tercero de MAGERIT, “Guía de técnicas“.

Análisis de Impacto de Negocio (BIA)

El análisis de impacto en el negocio (también conocido como BIA, por sus siglas en inglés Business Impact Analysis) tiene como principal objetivo identificar las necesidades del negocio en términos de recuperación. Sobre todo aquellas que consideramos como indispensables o “servicios mínimos” para el funcionamiento de la organización. Así pues, si realizamos este análisis, podremos contrastar las necesidades a las que nos hemos referido con la capacidad de recuperación de nuestros sistemas, lo que nos permitirá identificar las diferencias existentes y posteriormente, definir las estrategias de recuperación.

En el desarrollo del análisis de impacto en el negocio determinaremos cuales son los aspectos más importantes que pueden afectar a nuestro negocio y que pueden influir en la prestación de servicios a nuestros clientes. Asimismo, identificaremos los procesos o actividades críticas de negocio o BCA (Business Critical Activities).

Un aspecto importante a tener en cuenta en la elaboración de un BIA son los tiempos. En este sentido, cobran especial importancia los siguientes:

- RTO (Recovery Time Objective): Tiempo de recuperación de las actividades que hemos identificado bajo unas condiciones mínimas aceptables. Por ejemplo, supongamos que el Responsable del Departamento de Administración nos indica que, en caso de que fallara la plataforma que soporta las aplicaciones para la generación y emisión de la nómina, se deberían recuperar el servicio en un plazo máximo de 24h. En este caso, estableceríamos que el RTO asociado a dicho proceso es de 24h.
- MTD (Maximum Tolerable Downtime): Tiempo máximo tolerable de caída el cual nos determina el tiempo que puede estar caído un proceso antes de que se produzcan efectos desastrosos en la compañía y repercuta en el negocio. Volviendo al caso anterior, supongamos que el proceso de gestión de nóminas no debe estar interrumpido por un periodo superior a 48h. En este caso, estableceríamos que el MTD asociado a dicho proceso es de 48h.
- RPO (Recovery Point Objective): El grado de dependencia de la actualidad de los datos determina la cantidad máxima de información que se podría perder sin llegar a tener consecuencias inaceptables, formando parte de las políticas de respaldo definidas por la organización. En este sentido, imaginemos que el Responsable del Departamento de Administración nos indica que podrían tolerar una pérdida de información siempre y cuando no se perdieran los datos generados en más de un día completo. Por lo tanto, estableceríamos que el RPO es de 24h.

Por cada servicio o proceso analizado (generalmente no funciona bien a nivel de área completa, dado que servicios/procesos más críticos podrían arrastrar a otros menos críticos a definir medidas más restrictivas), se debería obtener la siguiente información:

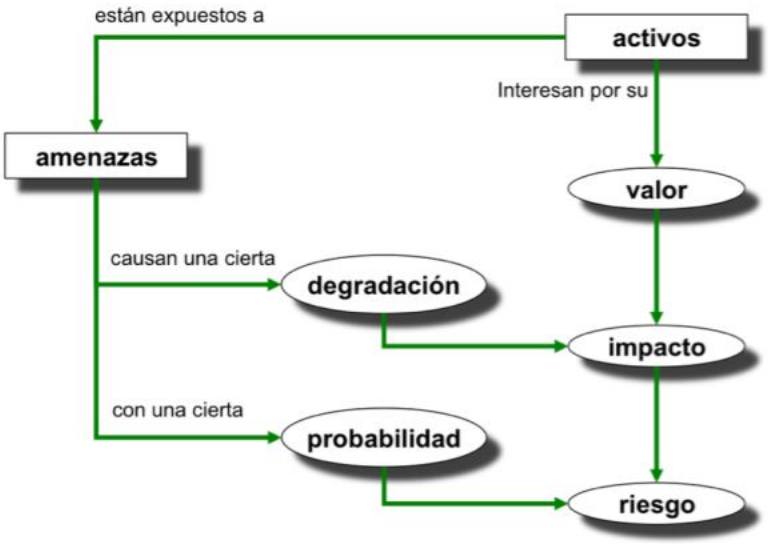
- Identificador y nombre del servicio/proceso.
- Descripción del mismo.
- Datos de contacto del responsable de negocio y técnico junto con sus backups.
- Procesos o servicios que dependen de este: Nombre e identificador, criticidad de la dependencia (p.e. baja, media o alta) y descripción de dicha dependencia.
- Procesos o servicios de los que depende este: Igual que el anterior.
- Las anteriores dependencias permitirán conocer el arbol de interrelaciones entre los servicios/procesos de la organización con el fin de evitar que, en caso de desastre, la falta de un servicio/proceso pueda poner en peligro otros que son críticos (en muchas ocasiones, servicios/procesos de soporte que podrían tener una baja criticidad por si mismos, pueden suponer un bloqueo en aquellos que si son críticos en caso de no haberse restaurado a tiempo).
- Proveedores críticos (externos a la organización): Proveedor, contacto, si existen ANS (Acuerdos de Nivel de Servicio) y los niveles establecidos.
- RTO, RPO y MTD.
- Matriz de impacto indisponibilidad servicio / proceso. En las filas las dimensiones de impacto (p.e. seguridad del servicio/proceso, imagen, costes, legislación y terceras partes) y en las columnas las dimensiones temporales (p.e. 1 hora, 1 día, 1 semana y 1 mes). Así, se podrá saber el impacto (p.e bajo, medio o alto) de cada periodo de indisponibilidad del servicio / proceso sobre cada dimensión como el daño de imagen o el impacto legal y regulatorio.

La información obtenida en la elaboración del BIA se validará con los distintos departamentos involucrados. Adicionalmente, contrastaremos los requisitos de recuperación con la capacidad de recuperación de los sistemas que intervienen en la prestación de servicios / procesos. En última instancia, se deberán presentar las conclusiones al comité de dirección para hacerlos partícipes y así obtener su respaldo de cara a afrontar nuevos proyectos para mejorar la capacidad de recuperación actual.

El BIA es un requisito básico de cara a la evaluación de riesgo, dado que nos permitirá entender mejor el impacto en la disponibilidad de las diferentes amenazas así como poder establecer salvaguardas acordes al impacto y a la criticidad de los diferentes servicios / procesos afectados.

Identificación de activos y amenazas

La evaluación del riesgo como proceso general, debe poder identificar y valorar los siguientes elementos:



La metodología MAGERIT V3 dispone de un catálogo donde se presentan los principales activos y amenazas (así como salvaguardas y criterios de valoración, que serán parte de otros capítulos).

Activos

El primer paso será identificar los activos, así como las amenazas que podrían impactar en los mismos y las vulnerabilidades que pueden ser explotadas para hacer realidad estas amenazas. A continuación veremos como se puede realizar el modelado de esto basada en la metodología MAGERIT v3 (metodología de acceso público creada para su uso en las administraciones públicas españolas y en las organizaciones privadas que les prestan servicios, y que se ha convertido en un estándar de facto en España).

En un sistema de información hay 2 cosas esenciales:

- la información que maneja
- y los servicios que presta.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

Subordinados a dicha esencia se pueden identificar otros activos relevantes:

- Datos que materializan la información.
- Servicios auxiliares que se necesitan para poder organizar el sistema.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos.

Por ello aparece como importante el concepto de “dependencias entre activos”. Se dice que un “activo superior” depende de otro “activo inferior” cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior.

Aunque en cada caso hay que adaptarse a la Organización objeto del análisis, con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores:

- activos esenciales:
  - información que se maneja.
  - servicios prestados.
- servicios internos:
  - que estructuran ordenadamente el sistema de información.
- el equipamiento informático:
  - aplicaciones (software).
  - equipos informáticos (hardware).
  - comunicaciones.
  - soportes de información: discos, cintas, etc.
- el entorno: activos que se precisan para garantizar las siguientes capas:
  - equipamiento y suministros: energía, climatización, etc.
  - mobiliario.
  - los servicios subcontratados a terceros.
  - las instalaciones físicas (edificios, CPDs, etc).

- el personal:
  - usuarios.
  - operadores y administradores.
  - desarrolladores.

Amenazas

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

El capítulo 5 del “Catálogo de Elementos“ (MAGERIT V3) presenta una relación de amenazas típicas.

- De origen natural: Hay accidentes naturales (terremotos, inundaciones, …). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.
  - Fuego.
  - Daños por agua.
  - Desastres naturales.
- Del entorno (de origen industrial): Hay desastres industriales (contaminación, fallos eléctricos, …) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.
  - Fuego.
  - Daños por agua.
  - Desastres industriales (explosiones, sobrecarga eléctrica, contaminación química, etc).
  - Contaminación mecánica como polvo, suciedad, vibraciones, etc.
  - Contaminación electromecánica: interferencias de radio, eléctricas, etc.
  - Avería de origen físico o lógico como fallos en equipos o programas.
  - Corte del suministro eléctrico.
  - Condiciones inadecuadas de temperatura y/o humedad.
  - Fallo de servicios de comunicaciones (intencionados o accidentales).
  - Interrupción de otros servicios y suministros esenciales como papel, toner, refrigerante, etc.
  - Degradación de los soportes de almacenamiento de la información.
  - Emanación electromagnética (que provoque que se puedan interceptar datos de forma remota, como leer emanaciones de una pantalla).
- Causadas por las personas de forma accidental: Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.
  - Errores de los usuarios.
  - Errores de los administradores.
  - Errores de monitorización como falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, etc.
  - Errores de configuración.
  - Deficiencias de la organización (cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión).
  - Difusión de software dañino (como malware, ransomware, etc).
  - Errores de (re-)encaminamiento en dispositivos de red.
  - Errores de secuencia (alteración accidental del orden de los mensajes transmitidos).
  - Escapes o fugas de información (llega a personas que no debería sin que se haya modificado, por ejemplo por envío de correo a destinatario incorrecto, incontinencia verbal).
  - Alteración accidental de la información.
  - Destrucción de información.
  - Vulnerabilidades de los programas (software).
  - Errores de mantenimiento / actualización de programas (software).
  - Errores de mantenimiento / actualización de equipos (hardware).
  - Caída del sistema por agotamiento de recursos (DoS/DDoS).
  - Pérdida de equipos.
  - Indisponibilidad del personal.
- Causadas por las personas de forma deliberada: Las personas con acceso al sistema de información pueden ser causa de problemas o ataques intencionados, bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.
  - Manipulación de los registros de actividad (log).
  - Manipulación de la configuración.
  - Suplantación de la identidad del usuario.
  - Abuso de privilegios de acceso.
  - Uso no previsto (juegos, consultas personales en internet, etc).
  - Difusión de sw dañino.
  - [Re-]encaminamiento de mensajes.
  - Alteración de secuencia.
  - Acceso no autorizado.
  - Análisis de tráfico (sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios).
  - Repudio (origen, recepción y/o entrega).
  - Interceptación de información (escucha).
  - Modificación deliberada de la información.
  - Destrucción de información.
  - Divulgación de información.
  - Manipulación de programas.
  - Manipulación de los equipos.
  - Denegación de servicio.
  - Robo.
  - Ataque destructivo (vandalismo, terrorismo, acción militar, etc).
  - Ocupación enemiga.
  - Indisponibilidad del personal.
  - Extorsión.
  - Ingeniería social.

Vulnerabilidades

Por desgracia, MAGERIT no incluye un catálogo de vulnerabilidades, dado que estas pueden ser muy variadas y una lista completa sería muy exhaustiva. Por ello, se recomienda trabajar con las amenazas y validar si por cada una de ellas que pueda afectar a la organización existen vulnerabilidades que las harían posibles.

Por ejemplo, en el caso de cortes de comunicaciones, una vulnerabilidad podría ser que el cableado de comunicaciones no está securizado, por lo que un atacante que lograse acceso físico podría cortar dicho cableado, o bien que

Desde el estándar ISO 27001 se dispone de un catálogo de vulnerabilidades generalista que podría servir como base para el trabajo (sirva más como ejemplo que como un catálogo completo):

- Interfaz de usuario complejas.
- Contraseñas predeterminadas no modificadas.
- Eliminación de medios de almacenamiento sin eliminar datos.
- Sensibilidad del equipo a los cambios de voltaje.
- Sensibilidad del equipo a la humedad, temperatura o contaminantes.
- Inadecuada seguridad del cableado.
- Inadecuada gestión de capacidad del sistema.
- Gestión inadecuada del cambio.
- Clasificación inadecuada de la información.
- Control inadecuado del acceso físico.
- Mantenimiento inadecuado.
- Inadecuada gestión de red.
- Respaldo inapropiado o irregular.
- Inadecuada gestión y protección de contraseñas.
- Protección física no apropiada.
- Reemplazo inadecuado de equipos viejos.
- Falta de formación y conciencia sobre seguridad.
- Inadecuada segregación de funciones.
- Mala segregación de las instalaciones operativas y de prueba.
- Insuficiente supervisión de los empleados y vendedores.
- Especificación incompleta para el desarrollo de software.
- Pruebas de software insuficientes.
- Falta de política de acceso o política de acceso remoto.
- Ausencia de política de escritorio limpio y pantalla clara.
- Falta de control sobre los datos de entrada y salida.
- Falta de documentación interna.
- Carencia o mala implementación de la auditoría interna.
- Falta de políticas para el uso de la criptografía.
- Falta de procedimientos para eliminar los derechos de acceso a la terminación del empleo.
- Desprotección en equipos móviles.
- Falta de redundancia, copia única.
- Ausencia de sistemas de identificación y autenticación.
- No validación de los datos procesados.
- Ubicación vulnerable a inundaciones.
- Mala selección de datos de prueba.
- Copia no controlada de datos.
- Descarga no controlada de Internet.
- Uso incontrolado de sistemas de información.
- Software no documentado.
- Empleados desmotivados.
- Conexiones a red pública desprotegidas.
- Los derechos del usuario no se revisan regularmente.

Valoración del riesgo

Una vez identificados los activos y las amenazas a los mismos, es necesario realizar una asignación de valores para los mismos, de forma que podamos saber el valor de un activo, la probabilidad e impacto de una amenaza, y con ello el nivel de riesgo de la organización.

Para ello nos basaremos en la metodología establecida por MAGERIT V3.

Valoración de activos

¿Por qué interesa un activo? Por lo que vale. No se está hablando de lo que cuestan las cosas, sino de lo que valen.

La valoración se puede ver desde la perspectiva de la ‘necesidad de proteger’ pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

El valor nuclear suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial.

Por otra parte, los sistemas de información explotan los datos para proporcionar servicios, internos a la organización o destinados a terceros, apareciendo una serie de datos necesarios para prestar un servicio. Sin entrar en detalles técnicos de cómo se hacen las cosas, el conjunto de información y servicios esenciales permite caracterizar funcionalmente una organización. Las dependencias entre activos permiten relacionar los demás activos con datos y servicios.

De un activo puede interesar calibrar diferentes dimensiones:

- su confidencialidad: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
- su integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.

- su disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios/procesos.

Adicionalmente, en sistemas dedicados a servicios de la sociedad de la información como puedan ser los de administración electrónica o comercio electrónico, el conocimiento de los actores es fundamental para poder prestar el servicio correctamente y poder perseguir los fallos (accidentales o deliberados) que pudieran darse. Así pues, en los activos esenciales, frecuentemente es útil valorar:

- la autenticidad: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada acción? Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar).
- la trazabilidad del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?
- la trazabilidad del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Una vez determinadas qué dimensiones (de seguridad) interesan de un activo hay que proceder a valorarlo. La valoración es la determinación del coste que supondría recuperarse de una incidencia que destrozara el activo.

Hay muchos factores a considerar:

- coste de reposición: adquisición e instalación.
- coste de mano de obra (especializada) invertida en recuperar (el valor) del activo.
- lucro cesante: pérdida de ingresos.
- capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas.
- sanciones por incumplimiento de la ley u obligaciones contractuales.
- daño a otros activos, propios o ajenos.
- daño a personas.
- daños medioambientales.

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles), como se verá más adelante. Los criterios más importantes a respetar son:

- la homogeneidad: es importante poder comparar valores aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra.
- la relatividad: es importante poder relativizar el valor de un activo en comparación con otros activos.

Casi todas las dimensiones mencionadas anteriormente permiten una valoración simple, cualitativa o cuantitativa. Pero hay una excepción, la disponibilidad. No es lo mismo interrumpir un servicio una hora o un día o un mes. Puede que una hora de detención sea irrelevante, mientras que un día sin servicio causa un daño moderado; pero un mes detenido suponga la terminación de la actividad de la organización. Y lo malo es que no existe proporcionalidad entre el tiempo de interrupción y las consecuencias (y ahí es donde entra el BIA).

Valoración de las amenazas

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

- Degradación (cuán perjudicado resultaría el valor del activo).
- Probabilidad (cuán probable o improbable es que se materialice la amenaza).

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto “totalmente degradado”, o “degradado en una pequeña fracción”. Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela de forma cualitativa por medio de alguna escala nominal (p.e alto, medio y bajo) o a veces (en organizaciones con una mayor madurez), de forma numérica (p.e asumiendo que 1 es 1 a vez al año de ocurrencia, 100 sería a diario o 1/100 cada siglo).

Determinación del impacto potencial

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios. Para enlazar unos con otros recurriremos al grafo de dependencias.

Impacto acumulado

Es el calculado sobre un activo teniendo en cuenta:

- su valor acumulado (el propio mas el acumulado de los activos que dependen de él).
- las amenazas a que está expuesto.

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada:

- El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo.
- El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

Impacto repercutido

Es el calculado sobre un activo teniendo en cuenta:

- su valor propio.

- las amenazas a que están expuestos los activos de los que depende.

  El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada:

- El impacto es tanto mayor cuanto mayor es el valor propio de un activo.

- El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.
- El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado.

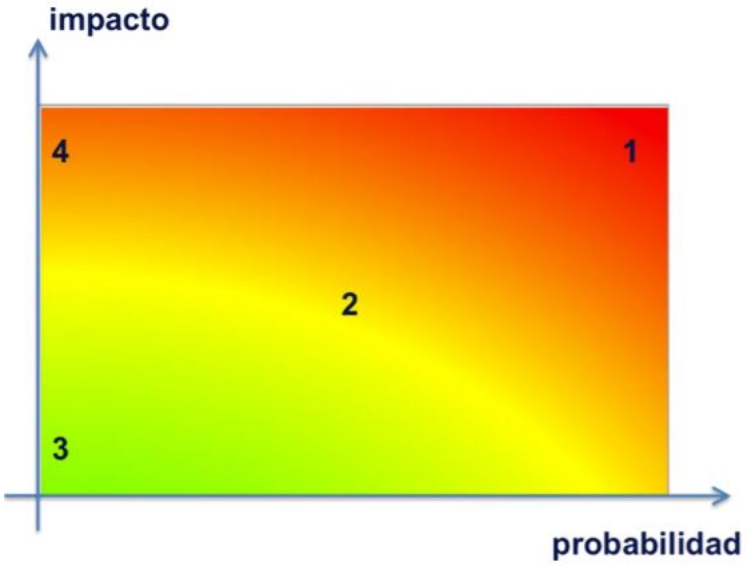
El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Determinación del riesgo potencial

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia. Por lo general se calcula multiplicando el impacto por la probabilidad, si bien para cada organización se puede adaptar esta formula.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo (que veremos más adelante):

- zona 1 – riesgos muy probables y de muy alto impacto.
- zona 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo.
- zona 3 – riesgos improbables y de bajo impacto.
- zona 4 – riesgos improbables pero de muy alto impacto.



Este modelo es un ejemplo basado en MAGERIT y puede ser adaptado a cada organización (con más o menos zonas). Este gráfico, con las amenazas incluidas se conoce como mapa de calor (permite visualizar los riesgos de la organización junto con sus impactos y probabilidades de forma sencilla y más entendible).

Riesgo acumulado

Es el calculado sobre un activo teniendo en cuenta:

- el impacto acumulado sobre un activo debido a una amenaza y
- la probabilidad de la amenaza.

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la probabilidad de la amenaza.

El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

Riesgo repercutido

Es el calculado sobre un activo teniendo en cuenta:

- el impacto repercutido sobre un activo debido a una amenaza y
- la probabilidad de la amenaza.

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la probabilidad de la amenaza.

El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Agregación de riesgos

Los párrafos anteriores determinan el riesgo que sobre un activo tendría una amenaza en una cierta dimensión.

Las organizaciones pueden utilizar la agregación de riesgos para juntar diferentes riesgos discretos o de bajo nivel dentro de un riesgo más general o de alto nivel. También se puede utilizar la agregación para gestionar eficientemente el alcance y escala de las evaluaciones del riesgo que involucran múltiples SI y áreas/servicios/procesos con relaciones específicas y dependencias entre dichos elementos.

La agregación debe realizarse bajo ciertas condiciones:

- Puede agregarse el riesgo repercutido sobre diferentes activos.
- Puede agregarse 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.
- Puede agregarse el riesgo de una amenaza en diferentes dimensiones.

Modelos de valoración de activos y del riesgo

De cara a valorar el valor de los activos, la probabilidad y el impacto de una amenaza, existen diferentes modelos que pueden ser aplicados:

- Modelos cuantitativos: Estos modelos se basan en asignar valores numéricos exactos (o en rangos determinados). Por ejemplo, una probabilidad de ocurrencia del 75%, un valor de 100.000 € o un impacto del 50% (de degradación). Estos modelos, si bien a priori parecen los más adecuados, requieren de un gran nivel de las organizaciones, y aún así es complicado en varios casos.
- Modelos cualitativos: Estos modelos se basan en asignar valores de entre un rango definido previamente como puede ser “alto / medio / bajo” o “muy alto / alto / medio / bajo / muy bajo”. Para ello las mediciones deben ser relacionadas teniendo en cuenta la comparación de los activos y las amenazas entre si, dado que en muchos casos el valor será relativo.
- Modelos semi-cuantitativos: Los análisis semi-cuantitativos se encuentran entre el cualitativo y cuantitativo dando como resultado valoraciones aproximadas en lugar de exactas o absolutas. Estos métodos son útiles cuando no se puede realizar mediciones o valoraciones directas y se acepta la posibilidad de realizar inferencias.

Por lo general, los metidos utilizados son el análisis cualitativo y cuantitativo, cada uno con sus ventajas e inconvenientes.

Métodos cuantitativos

Ventajas:

- Permite la definición de las consecuencias de un modo cuantitativo.
- Permiten el análisis de beneficio/coste durante la selección de las salvaguardas.
- Se obtiene una imagen mas ajustada de la valoración de riesgos.

Desventajas:

- Las medidas cuantitativas dependen del alcance y exactitud de las escalas de medida.
- El resultado del análisis puede ser no preciso y a veces confuso.
- Debe ser enriquecido con una descripción cualitativa.
- Suelen ser mas caros y requieren de mayor experiencia.

Métodos cualitativos

Ventajas:

- Permite determinar grandes áreas de riesgos en un corto periodo de tiempo y sin mucha experiencia.
- Suelen ser análisis mas fáciles y económicos.

Desventajas:

- No permite la estimación de probabilidades y resultados utilizando medidas numéricas.
- El análisis de coste/beneficio es mas difícil durante la fase de determinación de las salvaguardas.
- Los resultados son de carácter general mediante aproximaciones.

A continuación se muestran varios ejemplos de valores cualitativos:

- Probabilidad:
  - Muy alta (>90%) // Alta (Entre 60% y 90%) // Media (Entre 40% y 60%) // Baja (Entre 10% y 40%) // Muy baja (<10%).
  - 100 (diario) // 10 (mensual) // 1 (Anual) // 0,1 (Cada varios años) // 0,01 (Cada siglo).
- Valor e Impacto:
  - Muy alto (> 1M €) // Alta (Entre 700m € y 1M €) // Media (Entre 400m € y 700m €) // Baja (Entre 100m € y 400m €) // Muy baja (<100m €).
  - Alto (>100m €) // Medio (Entre 20m € y 100m €) // Bajo (<20m €).
- Impacto:
  - Alto (>75% degradación valor activo) // Alto (Entre 50 y 75% degradación) // Medio (Entre 30 y 50% degradación) // Bajo (Entre 10% y 30% degradación) // Muy bajo (<10% degradación).

Escenarios de riesgo

La estimación, prevención y reducción de riesgos es la clave para evitar pérdidas y desastres en cualquier organización. Uno de los pasos para lograr estos objetivos es la construcción de una serie de escenarios de riesgos, amenazas y vulnerabilidades. Su objetivo principal es tener una visión global de los riesgos, roles e interacciones para identificar prioridades en el tratamiento del riesgo.

Los escenarios son una herramienta poderosa para la gestión del riesgo, dado que ayudan a los profesionales a realizar las preguntas correctas y prepararse para lo inesperado. También permite introducir realismo, conocimiento interno, compromiso, análisis mejorado y estructura para la gestión del riesgo.

Un escenario de riesgo es una conceptualización de qué podría suceder a un área/servicio/proceso y que facilita analizar riesgos probables para la organización así como otros que sin ser probables, podrían tener un impacto enorme en la organización.

Para ello se pueden tomar dos aproximaciones:

- De arriba a abajo: En esta aproximación se comienza con los objetivos de negocio globales y se realiza un análisis de los escenarios de riesgos más probables y relevantes que podrían afectar a dichos objetivos.
- De abajo arriba: En esta aproximación se comienza con un conjunto genérico de escenarios (p.e. el listado de amenazas de MAGERIT al estilo de los checklists de amenazas, si bien, como se verá, este modelado va más allá) para definir escenarios más específicos y concretos para la organización.

Estas aproximaciones son complementarias y deberían usarse en conjunción. Estos escenarios deben ser relevantes y enlazados a los riesgos específicos de la organización.

Esta herramienta va más allá de las vistas anteriormente para la identificación y evaluación de riesgos, dado que permite modelar las amenazas y trabajar en ellas en profundidad para comprender mejor su impacto en la organización. Se trata de mucho más que obtener un listado de amenazas específicas, sino que se busca entender cómo el negocio podría ser impactado.

Comenzar a la vez por un listado genérico de escenarios permitirá que no se pasen por alto riesgos importantes, proveyendo a la vez una vista más comprensiva y completa del riesgo.

A continuación se muestra una aproximación práctica sobre cómo desarrollar estos escenarios:

- Comenzar con una lista genérica de riesgos para definir un conjunto inicial de escenarios para la organización.
- Validar dichos escenarios contra los objetivos del negocio.
- Refinar el conjunto de escenarios seleccionado basada en la validación anterior. Categorizarlos de forma que se alineen con la criticidad de la organización.
- Reducir el número de escenarios a un conjunto manejable.
- Mantener todos los riesgos en una lista de forma que puedan ser reevaluados en la siguiente iteración e incluidos para su análisis en detalle si se vuelven relevantes en ese momento.
- Incluir un “evento no especificado” en los escenarios para tratar los incidentes que no han sido cubiertos por los escenarios especificados.

Es importante que por cada escenario se especifique no sólo la amenaza, sino como la misma podría hacerse realidad en la organización. Se debe definir por cada uno el evento que lo produciría, cuándo y cómo sucedería.

Modelado de amenazas

El modelado de amenazas es un conjunto de técnicas que permiten analizar las potenciales amenazas que un desarrollo de software podría tener con el fin de asegurar que las mismas son tratadas mediante controles (ya sean implementados en el propio software como incluir cifrado a nivel de aplicación, o bien de forma externa, como cifrado a nivel de BBDD con la funcionalidad de esta).

Por ello, está íntimamente relacionado con el análisis de riesgos, ya que permite detectar posibles amenazas en una aplicación concreta con un nivel de grano fino, mucho más de lo que un análisis de riesgos general podría lograr.

El Modelado de Amenazas de Seguridad es un proceso para la evaluación y documentación de los riesgos de seguridad de un sistema. El modelado permite comprender el perfil de amenazas a las que está expuesto un sistema, mediante una evaluación a través de los ojos de sus potenciales enemigos. Con técnicas tales como la identificación de puntos de entrada, fronteras de privilegios y árboles de amenazas, se pueden identificar estrategias para mitigar las posibles amenazas del sistema.

El Modelado de Amenazas también permitirá la justificación de la implementación de las características de seguridad dentro del sistema, o las prácticas de seguridad para utilizarlo, para la protección de los activos de la organización.

Los pasos para crear un Modelo de Amenazas básicamente son los siguientes:

1. Crear una descripción de la arquitectura: Utilice diagramas y tablas para documentar la arquitectura, incluyendo sub-sistemas, fronteras de confianza (dónde la información abandona zonas que se consideran seguras, como una VLAN, a otras menos seguras, como la intranet o no seguras, como internet) y flujo de datos. Suele ser necesario la creación de diagramas de componentes físicos (servidores y componentes sw de alto nivel requeridos), así como diagramas de flujos de datos (como la información se mueve entre sistemas, así como dentro y fuera de la aplicación, ya sea con comunicación usuario-máquina o máquina-máquina a través de APIs).
2. Descomponer la aplicación: Descomponga la arquitectura de la aplicación, incluyendo la capa de red y el diseño de infraestructura, para crear un perfil de seguridad para la aplicación.
3. Identificar las amenazas: Utilice la información obtenida en los pasos 1 y 2 y la mentalidad de un atacante para identificar las amenazas más importantes para el contexto y el escenario del sistema.
4. Documentar las amenazas: Documente utilizando una plantilla que capture el conjunto básico de atributos de cada amenaza.
5. Asignar prioridades a las amenazas: Utilice una calificación de amenazas para centrarse en las áreas donde existe mayor vulnerabilidad y riesgo.

Para la identificación y documentación de las amenazas existen diferentes modelos. Uno de los más conocidos y utilizados es el modelo STRIDE creado por Microsoft (el primero de su clase).

Las amenazas se clasifican en las siguientes categorías que facilita en análisis de las potenciales amenazas de una aplicación (traducción al español de las siglas STRIDE):

- Suplantación de identidad de usuario (Spoofing).
- Modificación indebida (Tampering).
- Repudio (Repudiation).
- Divulgación de información (brecha de privacidad o filtración de información; Information Disclosure).
- Denegación de servicio (DoS).
- Elevación de privilegios (Elevation of Privileges).

Metodologías de análisis del riesgo

Si bien en este curso nos hemos centrado principalmente en la metodología MAGERIT para la evaluación del riesgo, existen otras metodologías que pueden ser utilizadas (también para la gestión del riesgo como el tratamiento y la monitorización:

- OCTAVE (Operationally Critical Threat Asset and Vulnerability Evaluation, desarrollado por el CERT en Carnegie Mellon University): Desarrollado en EEUU, es una metodología para recoger y analizar información de manera que se pueda diseñar una estrategia de protección y planes de mitigación de riesgo basados en los

riesgos operacionales de seguridad de la organización. Hay dos versiones, una para grandes organizaciones y otra para pequeñas, de menos de 100 empleados.
- MAGERIT: Metodología de análisis y gestión de riesgos de TI desarrollado por el Consejo Superior de Administración Electrónica y publicado por el Ministerio de Administraciones Públicas español, es una metodología de análisis de riesgos que describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación, detalla las tareas para llevarlo a cabo de manera que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión realmente efectivos.
- Estándar Internacional ISO/IEC 27005: La Norma habla de la gestión de los riesgos de la seguridad de la información de manera genérica, utilizando para ello el modelo PDCA, y en sus anexos se pueden encontrar enfoques para la realización de análisis de riesgos, así como un catálogo de amenazas, vulnerabilidades y técnicas para valorarlos.
- MEHARI: Método de análisis de riesgo que cuenta con un modelo de evaluación de riesgos y módulos de componentes y procesos. Con MEHARI se detectan vulnerabilidades mediante auditorías y se analizan situaciones de riesgo.
- CRAMM: CRAMM es la metodología de análisis de riesgos desarrollado por la Agencia Central de Comunicación y Telecomunicación del gobierno británico. El significado del acrónimo proviene de CCTA Risk Analysis and Management Method. Al igual que MAGERIT, tiene un alto calado en administración pública británica, pero también en empresas e instituciones de gran tamaño. Dispone de un amplio reconocimiento.
- NIST 800-30: Desarrollada por el Instituto Nacional de eStandares y Tecnología de EEUU. La norma NIST SP 800-30 nace con los siguientes objetivos: Aseguramiento de los sistemas de Información que almacenan, procesan y transmiten información // Gestión de Riesgos // Optimizar la administración de Riesgos a partir del resultado en el análisis de riesgos // Proteger las habilidades de la organización para alcanzar su misión (no solamente selacionada a la IT, sino de toda la empresa) // Ser una función esencial de la administración (no solo limitada a funciones técnicas de IT).

Informe de evaluación del riesgo

Este informe es el resultado del trabajo realizado durante la evaluación del riesgo.

Recoge todas las evidencias recopiladas y las conclusiones obtenidas sobre el entorno del riesgo (como los activos), las amenazas encontradas, su valoración en impacto y probabilidad y el mapa de riesgo de la organización.

A la vez este informe puede ser continuado en la siguiente fase incluyendo las salvaguardas existentes y a implementar junto con el riesgo residual tras la implementación de las mismas.

A continuación se muestran dos ejemplos del contenido que debería haber, el primero más simple, y el segundo más formal definido por la guía NIST 800-30.

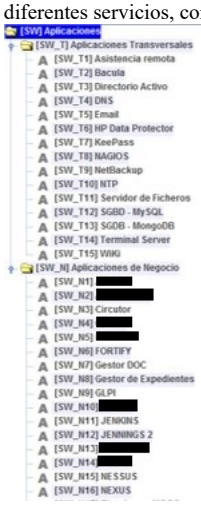
Plantilla simple

El contenido básico del mismo debería ser el siguiente:

- Descripción de los activos:
  - Descripción de los procesos de negocio o áreas junto con los servicios/procesos que cuelgan de los mismos y la información de cada uno de ellos.
  - Por cada una de las anteriores, árbol de activos con sus dependencias. En entornos complejos, describir los principales activos y sus dependencias, incluyendo así mismo la descripción de las categorías de activos existentes (en estos casos se recomienda el uso de una herramienta de análisis y gestión de riesgos donde se encuentre al información completa. incluyendo en el informe un resumen). Por ejemplo, en la herramienta PILAR (la herramienta asociada a la metodología MAGERIT), se pueden modelar las dependencias así:
    - A cada uno de los servicios/procesos e información manejada en los mismos se asigna una dependencia con las aplicaciones (transversales y de negocio) propias de cada uno de ellos, redes en la que se encuentran, almacenamiento y tratamiento de la información y personal correspondiente.
    - A su vez, estas aplicaciones poseen una dependencia directa con los servidores (físicos o virtuales) en los que se encuentran y su red correspondiente. Ambos parten del CPD, al igual que el resto de elementos de soporte.
    - La información manejada, que va a asociada a cada uno de los servicios/procesos, además de las dependencias propias del servicio, le corresponden aquellas relacionadas con el almacenamiento y backup de cada una de ellas.
    - De estas relaciones se crea un grado de dependencia respecto a la Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad que es heredado del valor asignado a cada servicio e información asociada
  - A modo de ayuda, se muestran una serie de ejemplos de cómo se puede presentar este árbol (definido bajo PILAR):
    - Primero se debería incluir el árbol con las diferentes áreas y los elementos de soporte de la organización:

    - A continuación, y por cada área de la organización, se mostrará la misma con sus servicios y la información asociada a los mismos (como ejemplo, se muestra el área de RRHH), describiendo los mismos:

- Por último, por cada elemento de soporte de los servicios, se mostrará su detalle (como ejemplo se incluyen los elementos de sw, tanto trasversales a diferentes servicios, como los asociados a cada servicio).



Incluir la relación entre los activos puede ser complejo salvo para organizaciones muy simples. Esto quedaría reflejado en la herramienta utilizada, si bien se pueden incluir algunos ejemplos (dejando claro que no se trata de los árboles de dependencia completos)

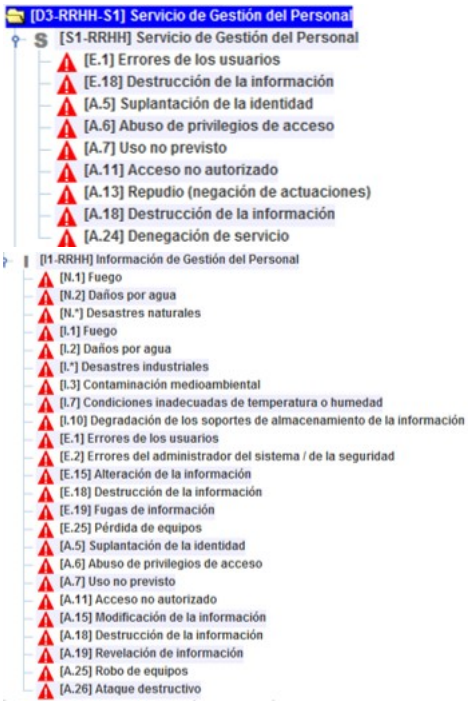
- A continuación se muestra el resumen del valor de los activos. En organizaciones complejas, se puede mostrar el valor agregado por áreas y cada servicio/proceso dentro de la misma. A continuación se muestra un ejemplo (la valoración para el valor en cada dimensión se realizó utilizando valores Alto, Medio y Bajo, y para el RTO y RPO en horas, días, mes):

Departamento	Servicio	Valoración						
		[C]	[I]	[D]	[A]	[T]	RTO	RPO
Unidad de Apoyo DG	Seguimiento y Reporte	A	A	A	A	A	H	H
	Gestión Relaciones Institucionales	B	A	B	A	A	D	D
Servicios Administrativos	Gestión Agenda	M	M	B	M	B	D	D
	Gestión Viajes y Gastos Organización	B	B	B	B	B	D	D
RRHH	Gestión de Personal	A	M	B	M	B	D	D
	Gestión de Formación	B	B	B	B	B	D	D
	PRL	B	B	B	B	B	D	D
Jurídico	Contratación sujeta a TRLCSP	B	M	M	M	B	D	D
	Contratación no sujeta a TRLCSP	M	M	M	M	B	D	D
	Información del Consejo, Socio Único, Estatutos y Escrituras	A	A	M	A	B	S	D

Como parte de esta sección, se detallarán los siguientes elementos:

- Descripción de los servicios/procesos críticos y la explicación de su criticidad.
- Descripción de las aplicaciones y elementos de soporte críticos (elementos de red, servidores de ficheros, etc) respecto a la disponibilidad, la integridad, la confidencialidad (por separado cada dimensión) y la trazabilidad. Incluir también la documentación en papel crítica (si la hubiese) respecto a la confidencialidad.
- Descripción de las redes críticas respecto a las diferentes dimensiones (p.e, autenticidad).

- Descripción del riesgo:
  - Descripción de las principales amenazas y su valoración: Realizar esta descripción a nivel de servicios/procesos, información, elementos de soporte (las tecnologías transversales, aplicaciones, redes, electrónica de red, los servidores, elementos de seguridad y almacenamientos, dado que sus amenazas son comunes), elementos de seguridad física, localizaciones (como el/los CPD) y las personas. A continuación se muestra un ejemplo para un servicio y su información.



- Descripción de los valores seleccionados para la probabilidad y degradación en las amenazas (metodología cuantitativa o cualitativa). A continuación se muestra un ejemplo cualitativo para la probabilidad y la degradación:

Potencial	Probabilidad	Nivel	Facilidad	Frecuencia
XL Extra Grande	CS Casi Seguro	MA Muy Alta	F Fácil	100
L Grande	P Probable	A Alta	M Medio	10
M Medio	PP Poco Probable	M Media	D Difícil	1
S Pequeño	I Improbable	B Baja	MD Muy Difícil	0,1
XS Muy Pequeño	MR Muy Raro	MB Muy Baja	ED Extremadamente Difícil	0,01

Nivel	Porcentaje
T - Total	100%
MA - Muy Alta	90%
A – Alta	50%
M – Media	10%
B – Baja	1%

- Mapas de riesgo:
  - Riesgo potencial: Este mapa refleja el nivel de riesgo al que estaría expuesto la organización respecto a parte de sus servicios y activos en caso de que no hubiera ningún tipo de salvaguarda implantada. Es por tanto un escenario simulado de riesgo, no real.
  - Riesgo presente: A continuación se muestra el nivel de riesgo al que está expuesto la organización respecto a sus servicios y activos con las salvaguardas existentes en la organización. Se trata de la situación actual.
    A continuación se muestra un ejemplo del riesgo potencial y riesgo presente a nivel de servicios e información:

- Debilidades (o vulnerabilidades): Descripción resumen de las principales debilidades encontradas por dominios (de la norma ISO 27001, como criptografía, seguridad de las comunicaciones, control de accesos, organización de la seguridad de la información, seguridad física y ambiental, gestión de activos, etc). A continuación se muestra un ejemplo para el dominio control de acceso:
  - La actual política no cubre todos los aspectos relativos al control de accesos, aunque incluye varias fichas específicas que suponen una base para la elaboración de futuros procedimientos.
  - No existe un procedimiento de gestión y registro de usuarios (básicos y privilegiados).
  - No existe un procedimiento específico para la gestión de privilegios donde se recojan los diferentes perfiles existentes, las revisiones de seguridad que se realizan y la periodicidad de las mismas.
  - No existen herramientas para automatizar el alta, baja y modificación de permisos de los usuarios de forma centralizada para permitir un acceso único unificado (de modo que una vez autenticado ante el sistema se pueda acceder a todas las aplicaciones y sistemas a las que se tengan permiso sin necesidad de ingresar otra vez el usuario y contraseña).
  - No hay ningún sistema que proteja el acceso de los administradores a sistemas, redes, dispositivos, aplicaciones y web administradas (acceso unificado, permisos de grano fino, monitorización de la actividad…).
  - El control de accesos implica el recordatorio de múltiples contraseñas.
  - No se dispone de mecanismos fuertes de protección y control de acceso a la información crítica, lo que podría llevar a fugas de la misma.
  - No se dispone de normativa ni procedimientos específicos para la gestión de contraseñas.
  - Existen aplicaciones “legacy” que no soportan un sistema centralizado de control de accesos.
  - No se han definido procesos periódicos de auditoría de los sistemas de autenticación, autorizaciones y privilegios de usuarios.
  - No se han definido un conjunto de métricas adecuado para evaluar la eficacia y eficiencia de los sistemas de gestión de usuarios y privilegios, ni están incorporados a un cuadro de mandos que permita una visión transversal de los sistemas.
- Anexo resumen áreas, servicios, valoraciones, red/es donde se encuentra la información, aplicaciones, herramientas y repositorios, información gestionada en general, dónde se encuentra localizada la información en papel, dónde se encuentra localizada la información digital y responsable del área. A continuación se

muestra un ejemplo para 2 áreas.

Departamento	Servicio	Descripción	Valoración				
			[C]	[I]	[D]	[A]	[T
Unidad de Apoyo DG	**Seguimiento y Reporte**	Seguimiento de toda la actividad y comunicación a Comités, Consejos, etc.	A	A	A	A	A
	Gestión Relaciones Institucionales	Comunicación, gestión y coordinación con instituciones ajenas a la Organización.	B	A	B	A	A
Servicios Administrativos	**Gestión Agenda**	Todas las funciones necesarias para el seguimiento y coordinación de la agenda de la Dirección.	M	M	B	M	B
	Gestión Viajes Y Gastos de la Organización	Trámites para realizar la gestión de los viajes de toda la Organización y gastos de la misma previo al paso a [redacted]	B	B	B	B	B

Plantilla NIST 800-30

El contenido será el siguiente:

- Resumen ejecutivo:
  - Fecha de la evaluación.
  - Resumen del propósito.
  - Descripción del alcance:
    - Para las capas 1 y 2 identificar las estructuras de gobierno o procesos asociados con la evaluación.
    - Para la capa 3 identificar los nombres de los sistemas de información y su localización, la categorización de seguridad y los limites (p.e autorización) de los mismos .
  - Si se trata de un análisis inicial o una actualización (y si es completa o incremental). En el segundo caso, describir el motivo que ha llevado a la actualización e incluir una referencia al informe previo.
  - Describir el nivel general de riesgo.
  - Listar el número de riesgos identificados por cada nivel (p.e. alto, medio y bajo).
- Cuerpo del informe:
  - Describir el propósito de la evaluación, incluyendo las preguntas que dicha evaluación debe responder.
  - Identificar las restricciones y asunciones.
  - Describir las entradas de tolerancia del riesgo para la evaluación (incluyendo el rango de consecuencias a ser considerado).
  - Identificar y describir el modelo de riesgo y la aproximación analítica utilizados. Proveer de una referencia (o incluirla como apéndice) identificando los factores de riesgo, las escalas de valores y los algoritmos para la combinación de valores.
  - Proveer el razonamiento para cada decisión relacionada con el riesgo durante la valoración.
  - Describir las incertidumbres del proceso y cómo han podido influir en el mismo.
  - Si el análisis incluye áreas de negocio, describir los servicios, interconexiones y dependencias, así como la TI que las soporta.
  - Si el análisis incluye SI de la organización, describir los sistemas, p.e. los servicios y áreas a los que da soporte, los flujos de información desde/a los sistemas y las dependencias con otros sistemas, servicios compartidos o infraestructuras comunes).
  - Resumir los resultados de la evaluación (p.e. mediante tablas o gráficos) de forma que permita a los decisores entender rápidamente el riesgo (p.e el número de eventos de riesgo para diferentes combinaciones de probabilidad e impacto y la proporción relativa de eventos de amenaza en diferentes niveles de riesgo).

    - Identificar el marco temporal durante el cual será valida la evaluación (p.e. el tiempo durante el cual los resultados podrán avalar la toma de decisiones).
    - Listar los riesgos debidos a amenazas de adversarios.
    - Listar los riesgos debido a otras amenazas.
- Apéndices:
    - Listado de referencias y fuentes de información.
    - Listado del equipo o personas individuales que han realizado la evaluación, incluyendo la información de contacto.
    - Listado de detalles de la evaluación y de cualquier evidencia de soporte, para facilitar el entendimiento y reutilización de los resultados.

Mitigación del riesgo

Introducción

A la vista de los impactos y riesgos a que están expuestos las áreas/servicios/procesos y los sistemas/aplicaciones (junto con todo el resto de infraestructura de soporte, localizaciones y personal), hay que tomar una serie de
decisiones condicionadas por diversos factores:

- La gravedad del impacto y/o del riesgo.
- Las obligaciones a las que por ley esté sometida la organización.
- Las obligaciones a las que por reglamentos sectoriales esté sometida la organización (banca, seguros, industrias críticas, etc).
- Las obligaciones a las que por contrato esté sometida la organización.

Dentro del margen de maniobra que permita este marco, pueden aparecer consideraciones adicionales sobre la capacidad de la Organización para aceptar ciertos impactos de naturaleza intangible tales como:

- Imagen pública de cara a la sociedad (aspectos reputacionales).
- Política interna: relaciones con los propios empleados, tales como la capacidad de contratar al personal idóneo, capacidad de retener a los mejores, capacidad de soportar rotaciones del personal, capacidad de ofrecer una carrera profesional atractiva, etc.
- Relaciones con los proveedores, tales como capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, capacidad de obtener trato prioritario, etc.
- Relaciones con los clientes o usuarios, tales como la capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia, etc.
- Relaciones con otras organizaciones, tales como la capacidad de alcanzar acuerdos estratégicos, alianzas, etc.
- Nuevas oportunidades de negocio, tales como formas de recuperar la inversión en seguridad.
- Acceso a sellos o calificaciones reconocidas de seguridad (ISO 27001, ISO 22301, CSA STAR, etc).

Todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo, determinándose si:

1. Es crítico en el sentido de que requiere atención urgente.
2. Es grave en el sentido de que requiere atención.
3. Es apreciable en el sentido de que pueda ser objeto de estudio para su tratamiento.
4. Es asumible en el sentido de que no se van a tomar acciones para atajarlo

La opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación. Las razones que pueden llevar a esta aceptación son:

- Cuando el impacto residual es asumible.
- Cuando el riesgo residual es asumible (y en esto hay que tener muy en cuenta riesgos con una probabilidad mínima, pero con un impacto gigantesco para la organización, para lo cual habría que estar preparado, por eso en este caso, el riesgo residual no sería asumible).
- Cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales.

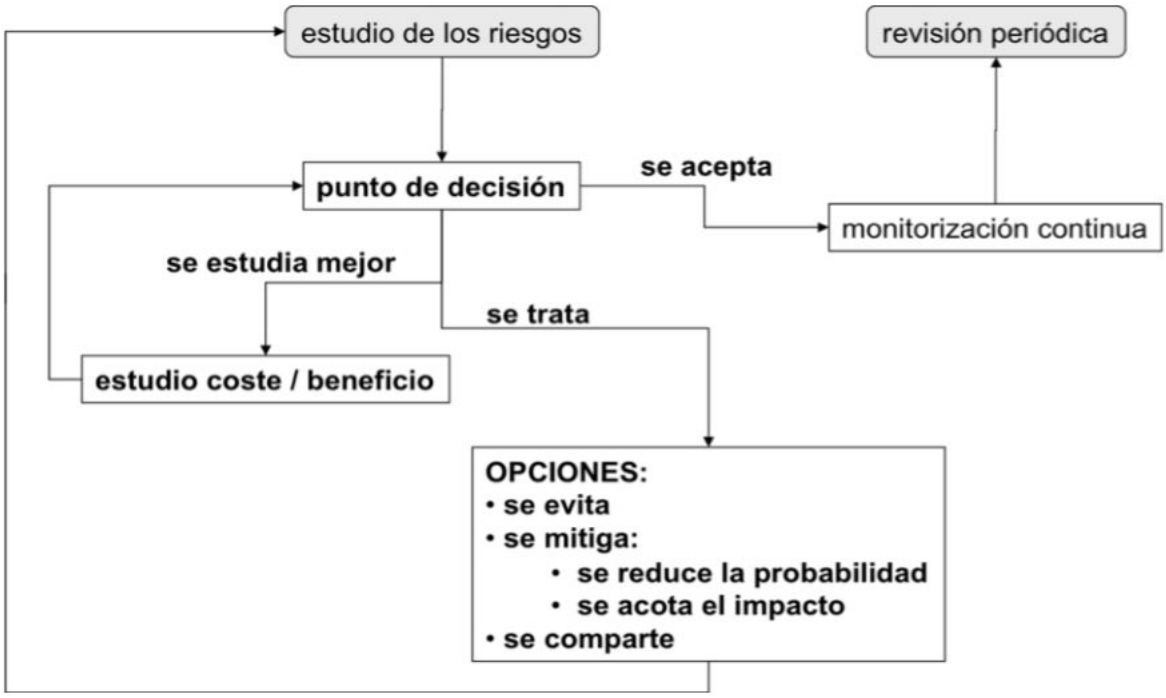
El análisis de riesgos determina impactos y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia. En cambio, el riesgo pondera la probabilidad de que ocurra. El impacto refleja el daño posible (lo peor que puede ocurrir), mientras que el riesgo refleja el daño probable (lo que probablemente ocurra).

El resultado del análisis es sólo un análisis. A partir de el disponemos de información para tomar decisiones conociendo lo que queremos proteger (activos valorados), de qué lo queremos proteger (amenazas valoradas) y qué hemos hecho por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo.

A partir de aquí, las decisiones son de los órganos de gobierno de la Organización que actuarán en 2 pasos:

1. Evaluación.
2. Tratamiento.

La siguiente figura resume las posibles decisiones que se pueden tomar tras haber estudiado los riesgos.



Para facilitar la aplicación de los conceptos que se verán en este capítulo, se ofrece a continuación un enlace al proyecto final de carrera de una alumna de ingeniería informática que realizó un ejemplo completo basado en la metodología MAGERIT V3 sobre una empresa real. Este ejemplo, junto con ejemplos más pequeños presentados en este capítulo facilitará obtener una visión práctica del tratamiento del riesgo, así como sobre la metodología MAGERIT en general. Se recomienda ver dicho documento de forma gradual tras obtener el conocimiento teórico para analizar su aplicación en la práctica.

Evaluación y tratamiento del riesgo

Para poder evaluar y tratar el riesgo, hay que entender una serie de conceptos, tanto para la propia evaluación como para poder determinar a posteriori la mejor opción para su tratamiento.

Interpretación de los valores de impacto y riesgo residuales

Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores aceptables.

Si el valor (impacto y riesgo) residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer.

Es importante entender que un valor residual es sólo un número. Para su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer y no se ha hecho; es decir, de las vulnerabilidades que presenta el sistema. Los responsables de la toma de decisiones deberán prestar cuidadosa atención a esta relación de tareas pendientes, que se denomina Informe de
Insuficiencias o de Vulnerabilidades (debilidades en el ejemplo presentado anteriormente del contenido de un informe de evaluación del riesgo).

Aceptación del riesgo

El comité de dirección, sometida al análisis de riesgos, debe determinar el nivel de impacto y riesgo aceptable.

Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias. Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión, …).

Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la dirección.

Cabe destacar que esta no es una opción de tratamiento del riesgo, per se, sino que el riesgo existente (o parte de el) es aceptado sin más por el motivo que sea.

Estos riesgos aceptados deberán ser monitorizados de forma continua y especial para asegurar que no cambien su valor (impacto y/o probabilidad, y puedan llegar a causar un impacto severo en la organización).

Tratamiento del riesgo

La dirección puede decidir aplicar algún tratamiento al sistema de seguridad desplegado para proteger el sistema de información. Hay dos grandes opciones:

- Reducir el riesgo residual (aceptar un menor riesgo).
- Ampliar el riesgo residual (aceptar un mayor riesgo).

Para tomar una u otra decisión hay que enmarcar los riesgos soportados por las áreas/servicios/procesos y sus aplicaciones/sistemas dentro de un contexto más amplio que cubre un amplio espectro de consideraciones de las que podemos apuntar algunas:

- Cumplimiento de obligaciones; sean legales, regulación pública o sectorial, compromisos internos, misión de la Organización, responsabilidad corporativa, etc.

- Posibles beneficios derivados de una actividad que en sí entraña riesgos.
- Condicionantes técnicos, económicos, culturales, políticos, etc.
- Equilibrio con otros tipos de riesgos: comerciales, financieros, regulatorios, medioambientales, laborales, etc.

En condiciones de riesgo residual extremo, casi la única opción es reducir el riesgo. En condiciones de riesgo residual aceptable, podemos optar entre aceptar el nivel actual o ampliar el riesgo asumido. En cualquier caso hay que mantener una monitorización continua de las circunstancias para que el riesgo formal cuadre con la experiencia real y reaccionemos ante cualquier desviación significativa.

En condiciones de riesgo residual medio, podemos observar otras características como las pérdidas y ganancias que pueden verse afectadas por el escenario presente, o incluso analizar el estado del sector en el que operamos para compararnos con la "norma".

En términos de zonas de riesgos (mapa de riesgos presentado anteriormente, también llamado mapa de calor), se pueden tomar las siguientes decisiones (mejores prácticas de la industria):

- Zona 1 – riesgos muy probables y de muy alto impacto; posiblemente nos planteemos sacarlos de esta zona.
- Zona 2 – riesgos de probabilidad relativa e impacto medio; se pueden tomar varias opciones.
- Zona 3 – riesgos improbables y de bajo impacto; o los dejamos como están, o permitimos que suban a mayores si ello nos ofreciera alguna ventaja o beneficio en otro terreno.
- Zona 4 – riesgos improbables pero de muy alto impacto; suponen un reto de decisión pues su improbabilidad no justifica que se tomen medidas preventivas, pero su elevado impacto exige que tengamos algo previsto para reaccionar; es decir, hay que poner el énfasis en medidas de reacción para limitar el daño y de recuperación del desastre si ocurriera.

También conviene considerar la incertidumbre del análisis. Hay veces que sospechamos las consecuencias, pero hay un amplio rango de opiniones sobre su magnitud (incertidumbre en el impacto). En otras ocasiones la incertidumbre afecta a la probabilidad. Estos escenarios suelen afectar a las zonas 4 y 3, pues cuando la probabilidad es alta, normalmente adquirimos experiencia, propia o ajena, con rapidez y salimos de la incertidumbre. En cualquier caso, toda incertidumbre debe considerarse como mala y debemos hacer algo:

- Buscar formas de mejorar la previsión, típicamente indagando en foros, centros de respuesta a incidentes o expertos en la materia.
- Evitar el riesgo cambiando algún aspecto, componente o arquitectura del sistema.
- Tener preparados sistemas de alerta temprana y procedimientos flexibles de contención, limitación y recuperación del posible incidente (de nuevo mediante la monitorización continua del riesgo).

A veces que estos escenarios de incertidumbre ocurren en un terreno en el que hay obligaciones de cumplimiento y la propia normativa elimina o reduce notablemente las opciones disponibles; es decir, el sistema se protege por obligación más que por certidumbre del riesgo.

Estudio del coste/beneficio

Es de sentido común que no se puede invertir en salvaguardas más allá del valor que queremos proteger.

Al avanzar de un grado de seguridad 0 hacia un grado de seguridad del 100%, el coste de la inseguridad (el riesgo) disminuye, mientras que el coste de la inversión en salvaguardas aumenta. Es intencionado el hecho de que el riesgo caiga fuertemente con pequeñas inversiones y que el coste de las inversiones se dispare para alcanzar niveles de seguridad cercanos al 100% (Regla de Pareto, normalmente con un 20% de las inversiones o del trabajo se puede lograr una cobertura del 80% del objetivo buscado).

Análisis cuantitativo

En la práctica, cuando hay que protegerse de un riesgo que se considera significativo, aparecen varios escenarios hipotéticos:

- E0: si no se hace nada.
- E1: si se aplica un cierto conjunto de salvaguardas.
- E2-N: si se aplican otros conjuntos de salvaguardas .

El análisis económico tendrá como misión decidir entre estas opciones, siendo E0 (seguir como estamos) una opción posible, que pudiera estar justificada económicamente.

En cada escenario hay que estimar a lo largo del tiempo el coste que va a suponer, teniendo en cuenta los siguientes elementos:

- Suma el coste del riesgo residual (recurrente).
- Suma el coste de las salvaguardas.
- Suma el coste anual de mantenimiento de las salvaguardas (recurrente).
- Resta al coste del análisis la mejora en la productividad.
- Resta al coste las mejoras en la capacidad de la organización para prestar nuevos servicios, conseguir mejores condiciones de los proveedores, entrar en asociación con otras organizaciones, etc (recurrente).

Estudio cualitativo

Cuando el análisis es cualitativo, en la balanza de costes beneficios aparecen aspectos intangibles que impiden el cálculo de un punto numérico de equilibrio.

Entre los aspectos intangibles se suelen contemplar:

- Aspectos reputacionales o de imagen.
- Aspectos de competencia: comparación con otras organizaciones de mismo ámbito de actividad
- Cumplimiento normativo, que puede ser obligatorio o voluntario.
- Capacidad de operar.
- Productividad.

Estas consideraciones nos llevan a contemplar diversos escenarios para determinar el balance neto. Por ejemplo, el no adoptar medidas puede exponernos a un cierto riesgo que causaría mala imagen; pero si la solución preventiva causa también mala imagen o supone un merma notable de oportunidades o de productividad, hay que buscar un punto de equilibrio, eligiendo una combinación de medidas que sea asumible.

Estudio mixto

En análisis de riesgos meramente cualitativos, la decisión la marca el balance de costes y beneficios intangibles, si bien siempre hay que hacer un cálculo de lo que cuesta la solución y cerciorarse de que el gasto es asumible. De lo contrario, la supuesta solución no es una opción. Es decir, primero hay que pasar el filtro económico y luego elegir la mejor de las soluciones factibles.

Opciones de tratamiento del riesgo

Si los riesgos no se aceptan será necesario tener una estrategia para tratarlos (respuesta al riesgo).

Eliminación

La eliminación de la fuente de riesgo es una opción frente a un riesgo que no es aceptable. En un sistema podemos eliminar varias cosas, siempre que no afecten a la esencia de la organización.

Es extremadamente raro que podamos prescindir de la información o los servicios esenciales por cuanto constituyen la misión de la organización. Cambiar estos activos supone reorientar la misión de la organización. Sin embargo, en determinados casos puede darse el caso de que el coste de otras opciones sea muy elevado frente al beneficio aportado por el activo amenazado, por lo que se decide prescindir del mismo (p.e de un servicio o proceso, de una actividad de negocio, etc).

Más viable es prescindir de otros componentes no esenciales, que están presentes simple y llanamente para implementar la misión, pero no son parte constituyente de la misma. Esta opción puede tomar diferentes formas:

- Eliminar cierto tipo de activos, empleando otros en su lugar. Por ejemplo: cambiar de sistema operativo, de fabricante de equipos.
- Reordenar la arquitectura del sistema (el esquema de dependencias) de forma que alteremos el valor acumulado en ciertos activos expuestos a grandes amenazas. Por ejemplo: segregar redes, desdoblar equipos para atender a necesidades concretas, alejando lo más valioso de lo más expuesto. etc.

Las decisiones de eliminación de las fuentes de riesgo suponen realizar un nuevo análisis de riesgos sobre el sistema modificado.

Mitigación

La mitigación del riesgo se refiere a una de dos opciones:

- Reducir la degradación causada por una amenaza (a veces se usa la expresión acotar el impacto).
- Reducir la probabilidad de que una amenaza de materializa.

En ambos casos lo que hay que hacer es ampliar o mejorar el conjunto de salvaguardas. En términos de madurez de las salvaguardas: subir de nivel.

Entre los tipos de salvaguardas, encontramos las siguientes tipologías (existen otros tipos de ordenamiento, pero desde el punto de vista de mitigación del riesgo nos interesa este):

- Salvaguardas preventivas: Buscan prevenir que una amenaza se haga real, por lo que disminuyen la probabilidad.
- Salvaguardas correctivas: Buscan minimizar el daño realizado en caso de materializarse la amenaza (disponer de un plan de recuperación ante desastres, copias de seguridad ante ransomware, sistemas de automatización de la respuesta ante incidentes de seguridad, etc), por lo que disminuyen el impacto
- Salvaguardas detectivas: Buscan detectar la ocurrencia de una amenaza. No modifican el impacto de forma directa, pero son necesarios para el funcionamiento de las salvaguardas correctivas.

Tras su depliegue hay repetir el análisis de riesgos, ampliándolo con los nuevos controles y, por supuesto, cerciorarse de que el riesgo del sistema ampliado es menor que el del sistema original; es decir, que las salvaguardas efectivamente disminuyen el estado de riesgo de la organización.

Más adelante en este capítulo veremos diferentes controles lógicos, físicos y administrativos para la mitigación de los riesgos.

Compartición o transferencia

Tradicionalmente se ha hablado de ‘transferir el riesgo’. Como la transferencia puede ser parcial o total, es más general hablar de ‘compartir el riesgo’.

Hay dos formas básicas de compartir riesgo:

- Riesgo cualitativo: se comparte por medio de la externalización de componentes del sistema, de forma que se reparten responsabilidades: unas técnicas para el que opera el componente técnico; y otras legales según el acuerdo que se establezca de prestación del servicio. En todo caso, es importante asegurar que le tercero al que se externaliza está cubierto frente a las amenazas que originaron el proceso y cómo. Así mismo, la responsabilidad legal no se externaliza del todo, puesto que seguimos siendo los propietarios del activo, servicio o proceso externalizado (por ejemplo de cara al RGPD), aunque luego se puedan exigir responsabilidades y compensaciones a la parte tercera (por incumplimiento de contrato).
- Riesgo cuantitativo: se comparte por medio de la contratación de seguros, de forma que a cambio de una prima, el tomador reduce el impacto de las posibles amenazas y el asegurador corre con las consecuencias. Hay multitud de tipos y cláusulas de seguros para concretar el grado de responsabilidad de cada una de las partes. En todo caso, es crítico conocer lo que se está contratando y el nivel de cobertura, puesto que en muchas ocasiones se descubre demasiado tarde que muchos aspectos no están cubiertos (p.e puede estar cubierto el cese de actividad, pero no los costes aumentados de personal para la recuperación). Así mismo, muchos seguros requerirán que existan un mínimo de controles de ciberseguridad antes de cubrir el riesgo de la seguridad de la información (y a partir de cierto nivel de control podría ayudar a disminuir el coste del seguro).

Cuando se comparten riesgos cambia, bien el conjunto de componentes del sistema o bien su valoración, requiriéndose un nuevo análisis.

Financiación (Aprovisionamiento)

Cuando se acepta un riesgo, la organización hará bien en reservar fondos para el caso de que el riesgo se concrete y haya que responder de sus consecuencias. A veces de habla de ‘fondos de contingencia’ y también puede ser parte de los contratos de aseguramiento. Normalmente esta opción no modifica nada del sistema y nos vale el análisis de riesgos disponible.

Cálculo de la disminución del riesgo

Una vez finalizado la evaluación del tratamiento y los controles a implementar (o riesgos aceptados, eliminados, transferidos), se deben generar los nuevos mapas de riesgo que muestren la situación de la organización tras su implementación (cuando estas estrategias son a más de 1 año, se recomienda generar mapas intermedios que muestren la mitigación del riesgo año a año).

El cálculo de la disminución en impacto y/o probabilidad no es sencillo. Generalmente se recomienda utilizar el sentido común, si bien existen herramientas para el análisis de riesgos que incluyen catálogos de controles con valores predeterminados, si bien estos se deberían editar cuando así se requiera para al organización (puesto que los entornos son diferentes entre diversas organizaciones, no siempre estos valores por defecto serán validos).

Requisitos de un programa de ciberseguridad

Esta sección trata de cómo llevar a cabo planes de seguridad, entendiendo por tales los proyectos que permitirán materializar las decisiones adoptadas para el tratamiento de los riesgos.

Estos planes reciben diferentes nombres en diferentes contextos y circunstancias:

- Plan de mejora de la seguridad.
- Plan director de seguridad.
- Plan estratégico de seguridad.
- Plan de adecuación.

Para ello se deberán realizar 3 tareas diferentes:

- Identificación de proyectos de seguridad.
- Plan de ejecución.
- Ejecución.

Identificación de proyectos de seguridad

En última instancia se trata de implantar o mejorar la implantación de una serie de salvaguardas
que lleven el impacto y el riesgo a los niveles residuales determinados por la Dirección. Este tratamiento de las salvaguardas se materializa en una serie de tareas a llevar a cabo.

Un programa de seguridad es una agrupación de tareas. La agrupación se realiza por conveniencia, bien porque se trata de tareas que en singular carecerían de eficacia, bien porque se trata de tareas con un objetivo común, bien porque se trata de tareas que competen a una única unidad de acción.

Cada programa de seguridad debe detallar:

- Su objetivo genérico.
- Las salvaguardas concretas a implantar o mejorar, detallando sus objetivos de calidad, eficacia y eficiencia
- La relación de escenarios de impacto y/o riesgo que afronta: activos afectados, tipos de activos, amenazas afrontadas, valoración de activos y amenazas y niveles de impacto y riesgo
- La unidad responsable de su ejecución.
- Una estimación de costes, tanto económicos como de esfuerzo de realización, teniendo en cuenta:
    - Costes de adquisición (de productos), o de contratación (de servicios), o de desarrollo (de soluciones llave en mano), pudiendo ser necesario evaluar diferentes alternativas.
    - Costes de implantación inicial y mantenimiento en el tiempo.
    - Costes de formación, tanto de los operadores como de los usuarios, según convenga al caso.
    - Costes de explotación.
    - Impacto en la productividad de la Organización.
- Una relación de subtareas a afrontar, teniendo en cuenta:
    - cambios en la normativa y desarrollo de procedimientos.
    - Solución técnica: programas, equipos, comunicaciones e instalaciones.
    - Plan de despliegue.
    - Plan de formación.
    - Una estimación del tiempo de ejecución desde su arranque hasta su puesta en operación.
- Una estimación del estado de riesgo (impacto, probabilidad y riesgo residual) a su finalización.
- Un sistema de indicadores (métricas) de eficacia y eficiencia que permitan conocer en cada momento la calidad del desempeño de la función de seguridad que se desea y su evolución temporal.

Las estimaciones anteriores pueden ser muy precisas en los programas sencillos; pero pueden ser simplemente orientativas en los programas complejos que conlleven la realización de un proyecto específico de seguridad. En este último caso, cada proyecto desarrollará los detalles últimos por medio de una serie de tareas propias de cada proyecto que, en líneas generales responderán a los siguientes puntos:

- Estudio de la oferta del mercado: productos y servicios.
- Coste de un desarrollo específico, propio o subcontratado.
- Si se estima adecuado un desarrollo específico hay que determinar:
    - La especificación funcional y no-funcional del desarrollo.
    - El método de desarrollo que garantice la seguridad del nuevo componente.
    - Los mecanismos de medida (controles) que debe llevar empotrados.
    - Los criterios de aceptación.
    - El plan de mantenimiento: incidencias y evolución.

Plan de ejecución

Hay que ordenar en el tiempo los proyectos de seguridad teniendo en cuenta los siguientes factores:

- La criticidad, gravedad o conveniencia de los impactos y/o riesgos que se afrontan, teniendo máxima prioridad los programas que afronten situaciones críticas.
- El coste del programa.
- La disponibilidad del personal propio para responsabilizarse de la dirección (y, en su caso, ejecución) de las tareas programadas.
- Las posibles dependencias entre proyectos. En muchos casos puede ocurrir que el comienzo de un proyecto dependa de la salida de otro/s. Por ejemplo, en el caso del despliegue de una salvaguarda técnica, puede ser necesario que se dispongan primero de los procedimientos y guías antes de poder acometer dicho proyecto (con el objetivo de asegurar el alineamiento del control técnico con los objetivos y requisitos organizacionales).
- Otros factores como puede ser la elaboración del presupuesto anual de la Organización, las relaciones con otras organizaciones, la evolución del marco legal, reglamentario o contractual, etc.

Típicamente, un plan de seguridad se planifica en tres niveles de detalle:

- Plan director: A menudo denominado “plan de actuación”, trabaja sobre un periodo largo (típicamente entre 3 y 5 años), estableciendo las directrices de actuación.
- Plan anual (una serie de planes anuales): Trabaja sobre un periodo corto (típicamente entre 1 y 2 años), estableciendo la planificación de los programas de seguridad.
- Plan de proyecto (un conjunto de proyectos con su planificación): Trabaja en el corto plazo (típicamente menos de 1 año), estableciendo el plan detallado de ejecución de cada programa de seguridad.

Se debe desarrollar un plan director único, que es el que da perspectiva y unidad de objetivos a las actuaciones puntuales. Este plan director permite ir desarrollando planes anuales que, dentro del marco estratégico, van estructurando la asignación de recursos para la ejecución de las tareas, en particular partidas presupuestarias. Y, por último, habrá una serie de proyectos que materializan los programas de seguridad.

Ejecución del plan

El objetivo de esta fase es el de alcanzar los objetivos previstos en el plan de seguridad para cada proyecto planificado.

Como salida del mismo tendremos lo siguiente:

- Salvaguardas implantadas.
- Normas de uso y procedimientos de operación.
- Sistema de indicadores de eficacia y eficiencia del desempeño de los objetivos de seguridad perseguidos.
- Modelo de valor actualizado.
- Mapa de riesgos actualizado.
- Estado de riesgo actualizado (impacto, probabilidad y riesgo residuales).

Informe de tratamiento del riesgo

El informe de tratamiento del riesgo incorpora las diferentes opciones de tratamiento del riesgo (riesgos aceptados, transferidos, eliminados y las salvaguardas a desplegar) junto con el mapa del riesgo tras su implementación. Este informe puede ser independiente o bien incluirse como continuación del informe de evaluación de riesgos.

Como mínimo debería contener la siguiente información:

- Introducción:
  - Fecha de ejecución.
  - Resumen del objetivo.
  - Descripción del alcance (relacionado con el informe de evaluación de riesgos y si el tratamiento afectará a todos los riesgos de la evaluación o una parte, definiendo en este segundo caso cuáles).
  - Objetivos estratégicos de seguridad. Descripción de los objetivos de seguridad a nivel estratégicos buscados con este plan de tratamiento. A modo de ejemplo se incluyen los siguientes:
    - Definición e implantación del Marco de Organización y Gestión de la Seguridad: Establecer la arquitectura organizativa de la Gestión de la Seguridad, establecer las funciones, roles y responsabilidades en el ámbito de la seguridad de sistemas de información, incluyendo las funciones de mantenimiento, seguimiento y control, abarcando la gestión de políticas, cuerpo normativo y, en su caso, procedimientos asociados.
    - Formación y concienciación del Personal en materia de Seguridad lógica: Asegurar que los usuarios, de todo tipo, son conscientes de las amenazas y riesgos en el ámbito de la seguridad de los sistemas de información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo.
    - Integridad de la Información: Mantener la información a salvo de modificaciones y/o borrados no autorizados (intencionados o no). El alcance de este objetivo incluye datos, sistemas, software de aplicación y auxiliar, así como la información que esté en soporte no digital y su gestión sea responsabilidad de Sistemas. Establecer Separaciones de Entornos y Segregación de Funciones. Segmentar y proteger las redes.
    - Confidencialidad de la Información: Limitar el acceso a la información de la organización de manera que solamente accedan las personas, procesos y medios autorizados. Establecer mecanismos de identificación y autenticación robustos y ajustados a las necesidades corporativas y de las Operaciones.
    - Disponibilidad de la Información: El objetivo principal es que la información esté disponible para quien, o para que, se necesite, en el momento y lugar oportunos y en el medio predeterminado adecuado. Para cumplir este objetivo las estrategias se basarán, preferentemente, en planes de recuperación y de contingencia.
    - Autenticidad: Es la propiedad de que una entidad es lo que afirma ser, quién dice ser o bien que garantiza la fuente de la que provienen los datos, de forma que se asegure el no repudio de las personas, dispositivos, servicios y entidades que acceden o procesan dicha información.
    - Trazabilidad: El objetivo principal es poder asegurar el histórico de creación, modificación y destrucción de la información, siguiendo procedimientos preestablecidos y autosuficientes a lo largo del ciclo de vida de la información y mediante la utilización de herramientas apropiadas.
    - Continuidad de negocio: Implementar los medios y procesos necesarios para que, en caso de desastre o contingencia grave, existan planes que permitan disminuir en lo posible los daños y perjuicios, de acuerdo al equilibrio coste de seguridad /riesgo aceptado.
    - Seguridad de Sistemas y componentes: Los elementos (Hardware y Software) que se usen para el tratamiento de la información estarán convenientemente certificados o asimilados con los niveles de seguridad recomendados, según su cometido, en normas y estándares reconocidos.
    - Clasificación e Inventario de los Activos de Información: Inventariar y clasificar los activos bajo la responsabilidad de TI, desde el punto de vista de la seguridad y de la gestión del riesgo.
    - Conocer y Gestionar los Riesgos de los Sistemas de Información: Mediante el uso de técnicas de análisis de riesgos conocer cuáles son los riesgos de los sistemas de información para, así, gestionarlos adecuadamente.
    - Creación de Sistemas de Información seguros: Incluir la seguridad en todo el ciclo de vida de los Sistemas de Información.
    - Seguridad de Redes de Datos: Diseñar las redes (tanto interna como externamente) de manera que se minimice la exposición frente a amenazas externas e internas. Fomentar el uso de arquitecturas seguras (segmentación, bastionado, etc.).
    - Análisis proactivo de vulnerabilidades: Ejecutar análisis de los sistemas y dispositivos con el fin de corregir vulnerabilidades conocidas, manteniendo los sistemas actualizados y evitando la materialización de las amenazas asociadas.
- Enfoque metodológico: Descripción del enfoque utilizado, incluyendo criterios de valoración, formulas, etc.
- Situación actual:
  - Debilidades: Detalle de las diferentes debilidades (vulnerabilidades) halladas por cada dominio de seguridad (de la ISO 27001). Se muestra un ejemplo a continuación.

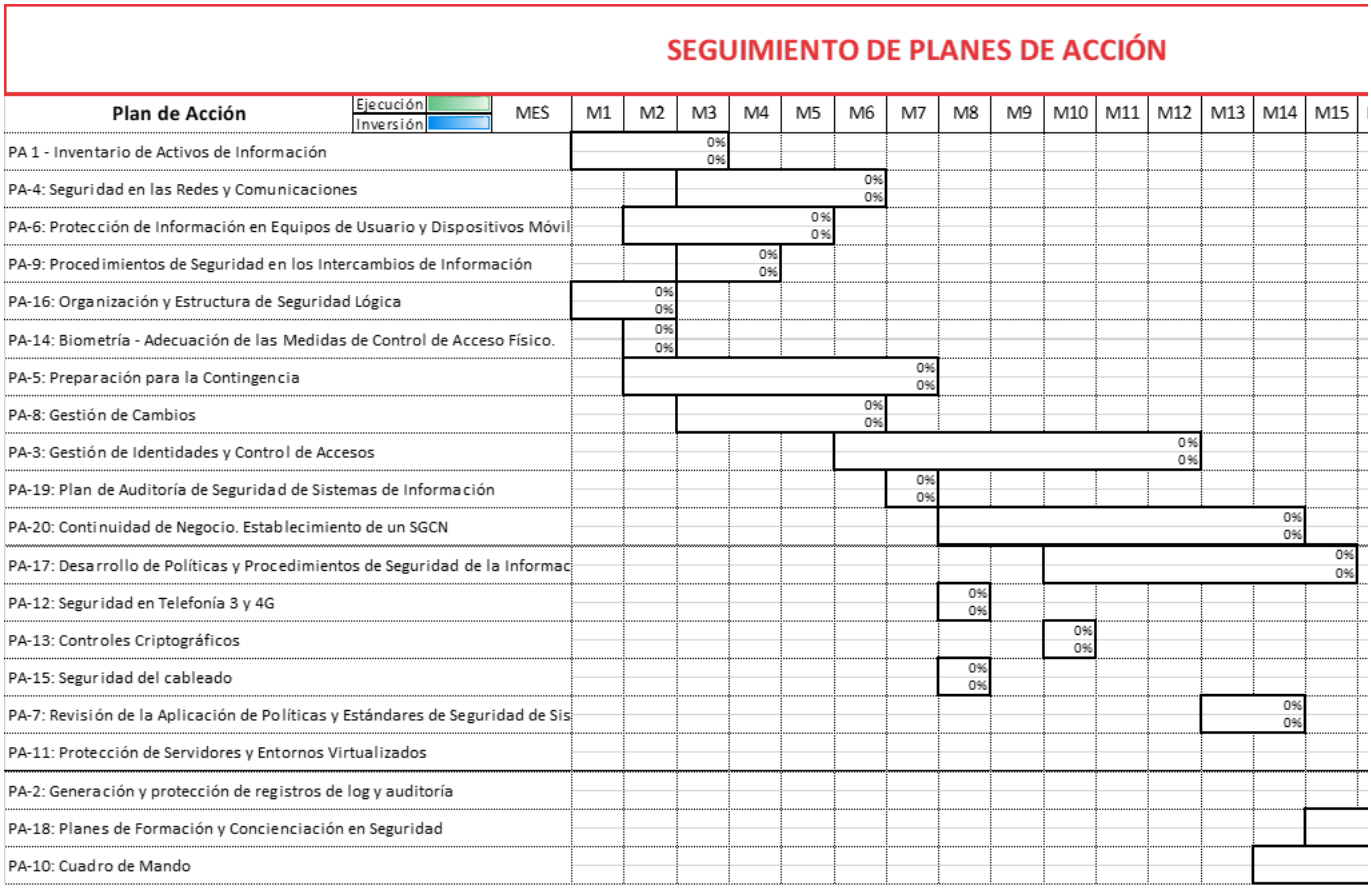
Organización de la seguridad	• El documento que recoge la actual estructura organizativa del SGSI es optimizable en concordancia con la política de seguridad. • No quedan definidos los diferentes comités y figuras de seguridad (personas, funciones, reuniones, periodicidad de las mismas y registros). • Con respecto a la segregación de tareas, no existen medidas de seguimiento sobre la adecuación de los puestos de trabajo y la colisión de responsabilidades. • No se han definido los requisitos de seguridad que se deben incluir en la gestión de cualquier tipo de proyecto. • La actual política sobre dispositivos móviles y teletrabajo queda incompleta. • No existe un procedimiento de seguridad de dispositivos móviles y teletrabajo, que recoja los criterios y controles que se deberán implantar para proteger la información de la empresa.
Seguridad en el Personal	• Aunque existen varios procedimientos para la gestión de recursos humanos, no queda definido un único procedimiento con todas las fases del ciclo de vida del trabajador: antecedentes, contratación y durante el empleo, cese y proceso disciplinario.
Gestión de activos	• No se dispone de un inventario de activos con responsables de los mismos. Por lo tanto, no existe una clasificación de activos en categorías (activos físicos, de servicios TI, de información y humanos). • Al no existir inventario, no se dispone de guías para la clasificación y valoración de activos, ni procedimientos para su realización y mantenimiento. • No existe una herramienta CMDB para el inventariado y gestión de activos. • No existe normativa ni procedimiento que recoja todo el tratamiento de los activos de información durante todo su ciclo de vida (clasificación, etiquetado, almacenamiento, difusión e intercambio, copias de seguridad y eliminación). • Aunque en la Normativa de Buenas Prácticas se dan una serie de indicaciones, no existen normativas ni procedimientos específicos que recojan las directrices para la gestión de soportes.

    - Mapas de riesgos: Incluir los mapas de riesgo presente así como el del riesgo final tras aplicar todas las salvaguardas (u otras opciones de tratamiento seleccionadas). En caso de que se trate de un proyecto a medio-largo plazo (2-3 años), se pueden incluir los mapas de riesgos de cómo quedaría la situación tras cada año (con las medidas implementadas de forma estimada en cada momento).
    - Resumen de los planes de acción: Descripción del periodo de implantación de las medidas (p.e definir qué se entiende por corto, medio y lago plazo) e incluir una tabla con el resumen de medidas y su plazo de implantación (siguiendo el ejemplo, corto, medio o largo plazo).
- Descripción en detalle de los planes de acción. Se pueden crear sub-capítulos por el tipo de planes que sean (seguridad lógica, física y administración y gestión de la seguridad). Por cada uno de los planes se detallará:
    - Descripción de la medida.
    - Objetivos concretos buscados.
    - Actividades a realizar.
    - Nivel de madurez buscado (por ejemplo en base al CMMi).
    - Entorno tecnológico involucrado (si lo hubiera).
    - Recursos necesarios (a nivel de personal y de inversión monetaria, explicitando cada elemento).
    - Métricas propuestas para la medición del plan.
- Acciones de monitorización necesarias: De acuerdo a lo establecido en el marco de gestión del riesgo de la organización y/o de forma ad-hoc. qué acciones son requeridas para monitorizar la implantación de los controles así como para valorar la disminución del riesgo en el tiempo.
- Apéndices:

- Resumen de los planes de acción. Por ejemplo en formato tabla con la información más relevantes por cada uno. Se incluye a continuación un ejemplo.

RESUMEN DEL PLAN DE ACCIÓN				
Nombre	**PA-5: Preparación para la Contingencia**			
Descripción	Diseñar, elaborar, implantar y ejercitar las medidas tecnológicas y procedimentales adecuadas para asegurar la contingencia de los servicios críticos y creando y entrenando los equipos con las personas necesarias para su operación y mantenimiento. Preparación del entorno de contingencias en XXX y cambios en el entorno de YYY (como la periodicidad de algunas copias de seguridad) para soportar las necesidades de disponibilidad de determinados servicios críticos.			
Ejecución	Plazo Comienzo	Corto	Prioridad	Media
	Tiempo Ejecución	6 Meses	Total Jornadas	80
	Coste HW & Lic.		# Perfiles	2
	Nivel CMM Actual	2	Nivel CMM Objetivo	4
Subproyecto	**Único**			
Acciones	1) Determinar los activos críticos para la organización que deben contar con un plan de contingencias			
	2) Obtener toda la información relevante de los activos críticos, incluyendo detalles de inventario, arquitectura, requerimiento legales, etc.			
	3) Analizar, para cada activo crítico, las posibles estrategias de respaldo.			
	4) Determinar, para el plan de contingencia de cada activo crítico los recursos necesarios, contemplando los recursos físicos, las necesidades de comunicaciones, la infraestructura de servidores y almacenamiento necesaria, el software y las copias de seguridad que habrán de estar disponibles, los recursos humanos y los procedimientos de activación, ejecución en contingencia, desactivación y vuelta a la normalidad			
	5) Analizar, una vez diseñados todos los planes necesarios, las sinergias que se pueden obtener entre ellos			

- Plan de proyecto con todos los proyectos necesarios, con fecha de inicio y fin. Se muestra un ejemplo a continuación (a 24 meses).
-



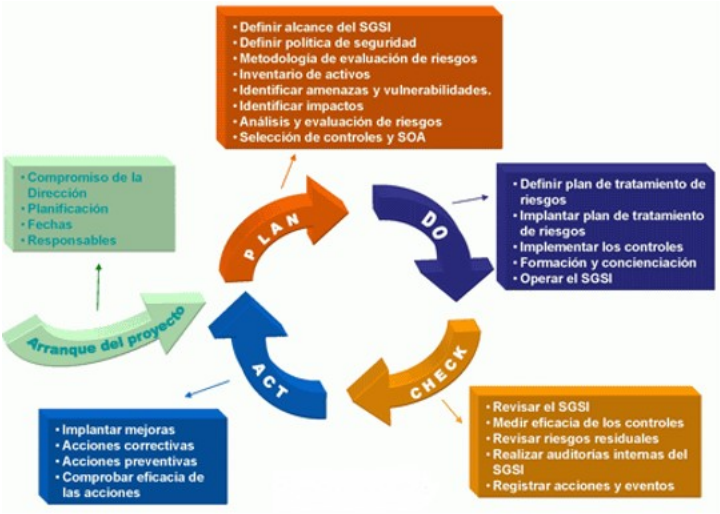
Frameworks de seguridad

Existen diferentes frameworks de seguridad de la información y ciberseguridad que nos permitirán contar con un conjunto de salvaguardas base entre las que poder escoger para los planes de mitigación del riesgo, así como establecer un marco general de gestión de la seguridad.

ISO 27001

LA norma ISO/IEC 27001 es un estándar para la seguridad de la información. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como “Ciclo de Deming”: PDCA, acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

Dado que el riesgo no es algo estático sino dinámico, un SGSI establecido bajo esta norma debe contemplar un proceso cíclico desarrollado en el ciclo PDCA:



La norma se encuentra dividida en dos partes; la primera se compone de 10 puntos entre los cuales se encuentran:

- Objeto y campo de aplicación: Especifica la finalidad de la norma, su uso dentro de una organización y el modo de aplicación del estándar.
- Referencias normativas: recomendación de la consulta a documentos necesarios para la aplicación del estándar.
- Términos y definiciones: Los términos y definiciones usados se basan en la norma ISO/IEC 27000.
- Contexto de la organización: Se busca determinar las necesidades y expectativas dentro y fuera de la organización que afecten directa o indirectamente al sistema de gestión de la seguridad de la información (SGSI). Adicional a esto, se debe determinar el alcance:
  - Entendiendo la organización y su contexto.
  - Entendiendo las necesidades y expectativas de los implicados.
  - Determinando el campo de aplicación del SGSI.
  - Sistema de gestión de la seguridad de la información.
- Liderazgo: Habla sobre la importancia de la alta dirección y su compromiso con el sistema de gestión, estableciendo políticas y asignando a los empleados de la organización roles, responsabilidades y autoridades, asegurando así la integración de los requisitos del sistema de seguridad en los procesos de la organización, así como los recursos necesarios para su implementación y operatividad.
- Planificación: Se deben valorar, analizar y evaluar los riesgos de seguridad de acuerdo a los criterios de aceptación de riesgos. Adicionalmente se debe dar un tratamiento a los riesgos de la seguridad de la información. Los objetivos y los planes para lograr dichos objetivos también se deben definir en este punto.
  - Acciones para abordar riesgos y oportunidades.
  - Objetivos de la seguridad de la información y cómo conseguirlos.
- Soporte: Se trata sobre los recursos destinados por la organización, la competencia de personal, la toma de conciencia por parte de las partes interesadas, la importancia sobre la comunicación en la organización. La importancia de la información documentada, también se trata en este punto.
- Operación: El cómo se debe planificar, implementar y controlar los procesos de la operación, así como la valoración de los riesgos y su tratamiento.
  - Planificación operacional.
  - Evaluación de riesgos.
  - Tratamiento de los riesgos.
- Evaluación de desempeño: Debido a la importancia del ciclo PDCA (Planificar, Hacer, Verificar, Actuar), se debe realizar un seguimiento, una medición, un análisis, una evaluación, una auditoría interna y una revisión por la dirección del SGSI del sistema de gestión de la información, para asegurar su correcto funcionamiento.
- Mejora: Habla sobre el tratamiento de las no conformidades, las acciones correctivas y a mejora continua.
  - Disconformidades y acciones correctivas.
  - Mejora continuada.

La segunda parte, esta conformada por el anexo A, el cual establece los objetivos de control y los controles de referencia (definidos en detalle en el estándar ISO 27002).

NIST CSF (Cyber Security Framework)

Este marco ayuda a las empresas de todos los tamaños a comprender, gestionar y reducir los riesgos de ciberseguridad y proteger sus redes, sistemas e información. Proporciona un lenguaje común y un resumen de las mejores prácticas en ciberseguridad.

Para abordar mejor estas amenazas, el presidente Obama emitió el 12 de febrero de 2013 la Orden Ejecutiva 13636: Mejora de la Ciberseguridad de las Infraestructuras Críticas. Esta demandó el desarrollo de un sistema voluntario de ciberseguridad (framework), un conjunto de estándares y mejores prácticas de la industria para ayudar a las empresas a gestionar los riesgos de ciberseguridad.

Este marco no provee nuevas funciones o categorías de ciberseguridad, sino recopila las mejores prácticas (ISO, ITU, CIS, NIST, entre otros) y las agrupa según afinidad. Se centra en el uso de impulsores de negocio para guiar las actividades de ciberseguridad y considerar los riesgos de ciberseguridad como parte de los procesos de gestión de riesgos de la organización. El framework consta de tres partes: el marco básico, el perfil del marco y los niveles de implementación.

- El Framework Core comprende un conjunto de actividades de ciberseguridad, resultados y referencias informativas que son comunes a través de los sectores de infraestructura crítica. Así, proporciona la orientación detallada para el desarrollo de perfiles individuales de la compañía.
- Mediante el uso de los perfiles, el marco ayudará a la organización a alinear sus actividades de ciberseguridad con sus requisitos de negocio, tolerancias de riesgo y recursos.
- Por su parte, los niveles de implementación del marco (tiers) proporcionan un mecanismo para que las empresas puedan ver y comprender las características de su enfoque para la gestión del riesgo de ciberseguridad.

Núcleo del marco

El núcleo proporciona cinco funciones continuas (Identificar / Detectar / Proteger / Responder / Recuperar). Asimismo, también brinda un conjunto de actividades para lograr resultados específicos de ciberseguridad y hace referencia a ejemplos de orientación para lograr esos resultados. El núcleo no es una lista de comprobación de las acciones a realizar. Presenta los resultados clave de ciberseguridad identificados por la industria como útiles para gestionar el riesgo cibernético.

A continuación se muestran las funciones y categorías (conjuntos de controles agrupados según afinidad) definidas por este marco:

FUNCIÓN IDENTIFICADOR ÚNICO	FUNCIONES	CATEGORÍA IDENTIFICADOR ÚNICO	CATEGORIAS
ID	IDENTIFICAR	ID.AM	Gestión de activos
		ID.BE	Ambiente de negocios
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	PROTEGER	PR.AC	Gestión de identidad, autenticación y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología de protección
DE	DETECTAR	DE.AE	Anomalías y Eventos
		DE.CM	Monitoreo continuo de seguridad
		DE.DP	Procesos de Detección
RS	RESPONDER	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
		RS.RP	Planificación de respuesta
RC	RECUPERAR	RC.RP	Planificación de la recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Níveles de implementación

Los *tiers* proporcionan un contexto sobre cómo una organización ve el riesgo de la ciberseguridad y los procesos implementados para manejarlo. Las escalas describen el grado en que las prácticas de gestión de riesgos de ciberseguridad de una empresa exhiben las características definidas en el marco. Por ello mismo, actúan como niveles de madurez en los procesos de ciberseguridad.

Los niveles de implementación caracterizan las prácticas de una compañía en un rango (4 niveles: parcial / riesgo informado / repetible / adaptativo). Estos niveles reflejan una progresión desde respuestas informales y reactivas hasta enfoques que son ágiles y están informados sobre el riesgo. Durante el proceso de selección de un *tier*, la empresa debe considerar sus actuales prácticas de gestión de riesgos, entorno de amenazas, requisitos legales y regulatorios, objetivos de negocio/misión y restricciones de organización.

Controles de mitigación: Seguridad administrativa

Gobierno de la ciberseguridad

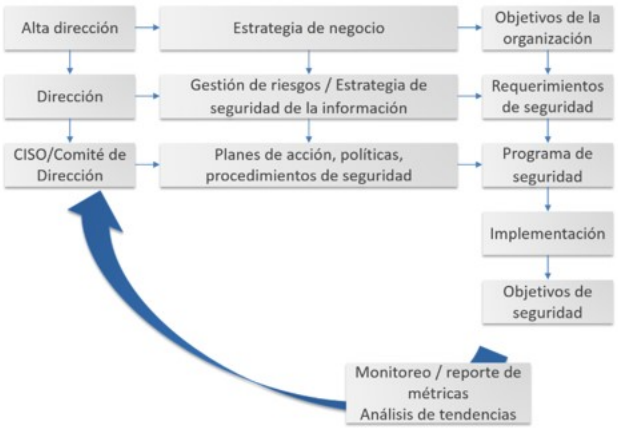
De acuerdo al modelo establecido por el IT Governance Institute (ISACA), la seguridad requiere la participación activa de los altos directivos de las empresas. El término que describe el compromiso de la alta dirección es el gobierno corporativo, que es el conjunto de responsabilidades y prácticas ejercidas por los responsables de una empresa (por ejemplo, el consejo y la alta dirección) con el objetivo de proporcionar dirección estratégica, asegurar que los objetivos sean alcanzados, garantizar que los riesgos sean gestionados adecuadamente, y verificar que los recursos de la empresa sean utilizados de manera responsable.

Por lo tanto, la ciberseguridad debe ser parte integral del gobierno corporativo para lograr sus objetivos, no sólo para cubrir las necesidades actuales sino también las futuras.

El objetivo de la seguridad de la información es desarrollar, implementar y administrar un programa de seguridad que alcance los siguientes cinco resultados básicos de un gobierno eficaz de seguridad:

1. Alineación estratégica: Alinear la seguridad de la información con la estrategia de negocio.
2. Administrar los riesgos: Ejecutar medidas apropiadas para mitigar los riesgos y reducir el posible impacto que tendrían en los activos de información.
3. Entrega de valor: Optimizar las inversiones en la seguridad.
4. Administración de recursos: Utilizar el conocimiento y la infraestructura de la seguridad de la información con eficiencia y eficacia.
5. Medición del desempeño: Monitorizar y reportar métricas de seguridad de la información para garantizar que se alcancen los objetivos.

Para lograr un gobierno eficaz, la alta dirección debe establecer un marco que guíe el desarrollo y mantenimiento de un programa integral de seguridad:



Esta figura muestra las relaciones y los participantes involucrados en el desarrollo de una estrategia de seguridad alineada a los objetivos de negocio. La estrategia tiene como entradas la estrategia de negocio, el estado actual y deseado de seguridad, los requerimientos del negocio y procesos, los resultados de la evaluación de riesgos y requisitos regulatorios. La estrategia proporciona la base para el desarrollo de los planes de acción (iniciativas de seguridad) en cumplimiento de los objetivos de seguridad.

Debido a que las organizaciones tienen diversas necesidades y sus enfoques de gobierno pueden variar, se ha identificado un conjunto básico de principios y buenas prácticas para ayudar a guiar estos esfuerzos.

Principios:

- El riesgo de seguridad de la información es más que un problema de TI: es un componente clave en la gestión de riesgos de la organización, lo que requiere la supervisión de la dirección.
- El riesgo tiene implicaciones legales que los directivos deben entender.
- El riesgo debe ser un tema de discusión en la junta de dirección de forma periódica.
- Los directores deben implementar un marco efectivo de gestión de riesgos en la organización.
- La alta dirección y el consejo deben evaluar el riesgo de seguridad de la información al igual que otros riesgos a nivel organizacional para asegurar que los riesgos se acepten, eviten, mitiguen o transfieran.

Buenas prácticas:

- Realizar una evaluación anual de la seguridad de la información a cargo de la alta dirección.
- Llevar a cabo evaluaciones de riesgos periódicos como parte de un programa global de gestión de riesgos.
- Implementar políticas y procedimientos basados en las evaluaciones de riesgos.
- Establecer una estructura de gestión de seguridad para asignar individualmente roles y responsabilidades.
- Desarrollar iniciativas para brindar seguridad de la información a redes, instalaciones, sistemas e información en general.
- Tratar la seguridad de la información como parte integral durante el ciclo de vida de los sistemas de información.
- Proporcionar concienciación, capacitación y educación en seguridad de la información para todo el personal.
- Conducir pruebas y evaluaciones periódicas para medir la efectividad de las políticas y procedimientos de seguridad de la información.
- Crear y ejecutar planes de acción para manejar cualquier deficiencia de seguridad de la información.
- Desarrollar e implementar procedimientos de respuesta a incidentes.
- Establecer planes, procedimientos y pruebas para proporcionar continuidad de las operaciones.
- Utilizar las mejores prácticas de la industria como ISO 27001, NIST SP 800, CoBIT, entre otros.

Políticas, procedimientos y guías

El cuerpo documental de la seguridad se compone de 3 patas (refinando las inferiores a las superiores):

- Políticas de seguridad: Las políticas de seguridad son documentos de alto nivel que establecen la visión de la dirección sobre la protección de los activos de la organización. Al ser de alto nivel, definen el qué, qué debe ser protegido, qué es más importante, qué es más prioritario, qué está permitido y qué no lo está y qué tratamiento se le darán a los problemas de seguridad. Su objetivo fundamental es proporcionar orientación y apoyo a la dirección para la seguridad de la información de acuerdo con los requisitos de la organización y con las regulaciones y leyes vigentes. Por ello, la dirección será quien establezca y promocione las políticas, demostrando su apoyo. En definitiva, se trata de unas guías de alto nivel que actuarán como paraguas bajo la que el resto de documentación de seguridad de la organización se agrupará y alineará (no pueden existir procedimientos y guías que no estén amparados por y desarrollen una política de seguridad, lo mismo que no debe haber políticas que no estén desarrolladas en detalle por procedimientos y guías).
- Procedimientos: Se trata de documentos que desarrollan a bajo nivel las políticas de seguridad pero de forma agnóstica a tecnologías concretas. Se deben definir los pasos a dar y, cuando sea posible, un flujograma que detalle las entradas y salidas, los pasos intermedios, los puntos de decisión y los resultados de dichas decisiones (como por ejemplo continuar a un siguiente paso o retornar a uno anterior para refinar el trabajo). Como ejemplo de estos podemos mostrar el procedimiento de altas, bajas y modificaciones de cuentas en los sistemas de información, el procedimiento de gestión de incidentes, etc.
- Guías: Estos documentos, los de más bajo nivel, muestran para cada tecnología concreta el cómo aplicar los procedimientos. No tiene porque haber una correspondencia exacta de un procedimiento a una guía, puesto que estas últimas pueden cubrir diferentes procedimientos para una tecnología concreta (como pueden ser las guías de configuración segura de SO y de Bases de Datos, que pueden cubrir aspectos como la generación de eventos y alertas de seguridad, configuración del cifrado de la información, el reforzamiento automático del control de acceso, etc). Sin embargo, es importante asegurar que todos los procedimientos estén cubiertos por una guía.

Con el objeto de desarrollar políticas de seguridad de calidad, debemos tener en cuenta varios aspectos:

- Adaptabilidad: La organización no debe adaptarse a un documento. La política debe adaptarse a los requerimientos de la organización. Por ello, se descarta la opción de copiar el documento de otra organización, más aún, si tenemos en cuenta que son diferentes los requerimientos de un tipo de organización de otra, como organismos públicos o privado, o del sector industrial y de banca.
- Definición de los objetivos: El documento precisa definir los objetivos de seguridad de la información, su forma de aprobación y la manera en que han de ser revisados, sin entrar en detalles acerca de estos procesos.

- Compromiso: La Alta Dirección de la organización debe expresar sin lugar a dudas, su compromiso total con el sistema y con su propósito final, que no debe ser otro que cumplir con los requerimientos en materia de seguridad de la información de las partes interesadas en el sistema.
- Comunicación: El documento debe establecer quién o quiénes son los encargados de comunicar a las partes interesadas los alcances y la evolución del sistema, no solo durante la implementación del mismo, sino en adelante, en la medida en que se presenten revisiones, actualizaciones o mejoras.
- Revisiones_ La política de Seguridad de la Información debe ser revisada en forma periódica, y estas revisiones, así como los responsables de las mismas, y los periodos de tiempo en los que se efectuarán, son temas que se deben incluir en el documento.
- Alineamiento legal, regulatorio y normativo. Dado que las leyes y regulaciones, tanto generales como sectoriales, son de obligado cumplimiento, se hace vital que las políticas de seguridad estén alineadas con las mismas y desarrollen su cumplimento dentro de la organización. Así mismo, existen normas sectoriales que no son publicadas por el gobierno, pero si pueden ser de obligatorio cumplimiento dentro de dicho sector, como puede ser el estándar de seguridad de datos para la protección de información de tarjetahabientes promovido por las grandes empresas de tarjetas de pago a nivel mundial (el consorcio PCI compuesto por miembros como VISA, MasterCard o American Express).

De acuerdo a las buenas prácticas dela industria, una política de seguridad debería incluir los siguientes puntos:

- Introducción: Breve explicación del asunto principal de la política.
- Ámbito de aplicación: Descripción de los departamentos, áreas o actividades de una organización a las que afecta/aplica la política. Cuando es relevante en este apartado se mencionan otras políticas relevantes a las que se pretende dar cobertura desde ésta.
- Objetivos: Descripción de la intención de la política.
- Principios: Descripción de las reglas que conciernen a acciones o decisiones para alcanzar los objetivos. En algunos casos puede ser de utilidad 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 responsable de qué acciones para cumplir con los requisitos de la política. En algunos casos, esto puede incluir una descripción de los mecanismos organizativos, así como las responsabilidades de las personas con roles designados.
- Resultados clave: Descripción de los resultados relevantes para las actividades de la organización que 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.

Finalmente, las políticas de seguridad más típicas en una organización serían las siguientes:

- Gestión de activos: Inventariado y gestión del ciclo de vida de los activos.
- Clasificación de la información: Guía de alto nivel sobre los niveles de clasificación de la información en la organización y cómo catalogar la misma de acuerdo a los criterios establecidos.
- Uso aceptable: Qué entiende la organización por uso aceptable de los diferentes activos aportados por la misma a los usuarios (por ejemplo, medios extraíbles, ordenadores, smartphones, etc).
- Control de Acceso: Guías de alto nivel sobre la gestión de identidades y control de acceso (como por ejemplo, el tipo de control de acceso a utilizar en base a criterios como la clasificación de la información accedida).
- Seguridad para proveedores: Criterios generales para asegurar que los proveedores con acceso a nuestros sistemas y/o información (ya sea de forma remota o en sus instalaciones) cumplen con un mínimo de requisitos que aseguren un nivel de seguridad adecuados.
- Continuidad de negocio: Establecer los parámetros generales para la continuidad de negocio en caso de un desastre y asegurar la recuperación de sistemas y servicios en un tiempo razonable que minimice el impacto a la organización a la vez que el coste.
- Gestión de incidentes: Criterios generales para asegurar que en caso de incidente se disponen de los medios y conocimiento necesario para detectarlo, investigarlos y priorizarlos, contenerlos, resolverlos y recuperar el entorno.
- BYOD: Criterios generales para el uso razonable de dispositivos personales de comunicación (como smartphones) para el acceso y trabajo con al información de la organización (en caso de aceptarse dicho uso).
- Dispositivos móviles y teletrabajo: Criterios generales para asegurar la seguridad en el uso de dispositivos móviles aportados por la organización (como smartphones y portátiles), así como cuando se esté teletrabajando.
- Gestión de claves y certificados: Criterios generales para la gestión del ciclo de vida de los certificados, tanto los emitidos internamente como los adquiridos externamente, desde su creación a su revocación.
- Eliminación y destrucción de la información: Criterios generales para la eliminación y destrucción de información en papel o digital, así como para la retirada de medios de almacenamiento (como discos duros o cintas de backup) en base a la clasificación de la información contenida.
- Escritorios y pantallas limpios: Requisitos para el uso de información en el espacio de trabajo individual o colectivo (hot sites) para evitar robo u espionaje.
- Gestión del cambio: Criterios de seguridad a introducir en el proceso de gestión del cambio para asegurar que el mismo se realiza de forma segura, incluyendo aspectos como la aprobación, prueba de los mismos en entornos previos a producción en caso de posibles impactos a la seguridad, existencia de planes de vuelta atrás en caso de problemas, etc.
- Copias de seguridad: Criterios generales sobre copias de seguridad de acuerdo a la clasificación de la información, teniendo en cuenta aspectos como la periodicidad, tipología (completos, incrementales, etc), periodo de retención, pruebas, etc.
- Transferencia de información: Criterios generales para asegurar la información cuando es transferida, tanto mediante correos electrónicos como mediante procesos automatizados.

A continuación se puede encontrar varias plantillas (en inglés) sobre diferentes políticas de seguridad, cortesía del instituto SANS: https://www.sans.org/security-resources/policies
También las guías de políticas para PYMES del INCIBE (en español): https://www.incibe.es/protege-tu-empresa/herramientas/politicas

Organización de la seguridad de la información

Para poder responder de forma eficaz y eficiente a los retos de la seguridad de la información en la organización, se deben organizar y estructurar las responsabilidades y las funciones relacionadas con la seguridad, así como asegurar que no existan lagunas.

El objeto es describir y documentar la estructura de responsabilidades, competencias y relaciones relativas a la seguridad de la información en la organización.

Funciones y responsabilidad de la seguridad de la información

Se trata de definir las responsabilidades de cada empleado o puesto de trabajo en relación a la Seguridad de la Información. Es decir, sumar a las funciones de cada puesto aquellas funciones que tengan que ver con la seguridad de la información (si es pertinente)

Pero no basta con definirlas, también deberemos comunicar a cada persona implicada en la Seguridad de la Información sus roles y responsabilidades

También se deben incluir a terceras partes, dado que son una parte crítica del proceso en muchas ocasiones.

Para terminar de cumplir con este control siempre que sea aplicable, deberemos procurar hacer partícipes de las responsabilidades a las partes externas que sean pertinentes tales como:

- Usuarios externos.

- Proveedores.
- Etc.

Segregación de tareas

Se trata de evitar usos o accesos indebidos a la información o a las aplicaciones o sistemas que la gestionan (activos de información) mediante la separación de las funciones asignando distintos perfiles o áreas de responsabilidad

Explicado de otra forma, podemos determinar las responsabilidades, tareas, accesos, etc. que conllevan un riesgo de mal uso, accidental o deliberado, si son compartidas por una misma persona.

Así, se debe crear una matriz SoD (Segregación de funciones en sus siglas en inglés), con los diferentes roles existentes y las funciones, asignando quién puede hacer qué, y sobre todo, determinando que funciones son incompatibles para un mismo rol (de forma que, en caso de querer realizar un fraude o acción ilícita en general, se deba, obligatoriamente, requerir de colusión, es decir, que 2 o más roles deban ponerse de acuerdo para realizar dichas tareas, p.e, que quien solicita un gasto sea diferente de quien lo aprueba).

A veces por motivos de costes no podemos diferenciar las responsabilidades o tareas. Entonces la pregunta es ¿qué podemos hacer si nuestra organización es demasiado pequeña y no tenemos más remedio que concentrar funciones en las mismas personas?

La alternativa está en establecer controles que mitiguen los riesgos provocados por la imposibilidad práctica de segregar las funciones:

- Controles de seguimiento y monitorización: Establecer controles de supervisión de las actividades en tiempo real puede darnos mayor seguridad de que se realizan correctamente (por ejemplo, establecer alarmas cuando determinadas tareas sensibles sean ejecutadas).
- Controles de Auditorias: Establecer controles mediante registros que revelen los datos necesarios en las auditorias periódicas para evaluar las posibles violaciones de seguridad. También es aconsejable aumentar la frecuencia de las auditorias en temas sensibles con el objeto de transmitir a los empleados la continuidad en la vigilancia de la seguridad de la información.
- Registros automatizados: Registrar de forma automática los cambios, accesos o tareas sensibles con la seguridad de la información como la asignación de permisos, contraseñas o modificaciones en aplicaciones de desarrollo.

Contacto con autoridades

En caso de incidentes en la seguridad de la información, puede resultar necesario mantener informados a los organismos de control del estado o administración. Estos pueden ser comúnmente:

- Agencia de protección de datos
- Fuerzas y Cuerpos de seguridad del estado
- Otros (como comunidades de ciber-inteligencia en las que la organización participe).

Así, se deberán establecer dentro de los procedimientos de gestión de incidentes a quién se contactará, cuándo se realizará el contacto, los datos de contacto de los grupos necesarios y la información que se deberá transmitir (con el objeto de ser tanto efectivos como evitar proporcionar más información de la realmente necesaria).

Contacto con grupos de interés especial

Mantenerse al día en seguridad de la información parece una tarea imposible de realizar de forma autónoma, aun para grandes corporaciones, por lo que este control nos indica que deberemos identificar todos aquellos grupos de interés tales como: foros especializados en Seguridad de la información, organismos administrativos como INCIBE en España o empresas expertas en seguridad de la información.

Se trata de mantenernos actualizados en cuanto a las noticias sobre la seguridad de la información y permanecer alerta ante las nuevas amenazas para la seguridad de la información y si es necesario que adoptemos alguna recomendación de estos grupos especializados.

Seguridad de la información en la gestión de proyectos

Este control pretende decirnos que la seguridad de la información debe involucrarse en todos los procesos de la organización ya sean procesos del negocio, procesos internos, servicios o productos, procesos TI etc.

Para afrontar este requisito es necesario realizar una evaluación de riesgos, centrada en la seguridad de la información, al comienzo de cualquier proyecto, para identificar amenazas, vulnerabilidades y riesgos asociados al proyecto. Esto nos permitirá adoptar los controles necesarios.

Para ello, se puede establecer el siguiente proceso (integrado dentro del marco de gestión del riesgo organizacional):

1. Objetivos de Seguridad: Plantear como una actividad más dentro de las actividades de cualquier proyecto el determinar los objetivos para preservar la confidencialidad, integridad y disponibilidad de la información relacionada o afectada por el proyecto.
2. Evaluación de riesgos: En la fase de diseño o planificación del proyecto se puede realizar un análisis de riesgos que nos permita identificar y ponderar los riesgos asociados a la seguridad de la información.
3. Controles de seguridad: La evaluación de riesgos nos permitirá tomar las decisiones adecuadas para establecer los controles necesarios para mitigar los riesgos en cada proyecto.
4. Proceso de Seguridad de la Información: Una vez que hemos realizado un ejercicio según los pasos anteriores podemos entonces establecer un proceso documentado para integrar la seguridad de la información en cualquier proceso con el conocimiento de lo que hemos aprendido.

Beneficios de la integración de la seguridad de la información en los proyectos:

- Cumplir con los requisitos de las leyes, regulaciones, estándares, normas, etc.
- La consideración de la seguridad de la información en todos los proyectos otorgara un mayor valor a todos los proyectos y a toda la organización.
- Mejora la evaluación de costes de un proyecto al considerar anticipadamente riesgos, que después pueden suponer costes no evaluados.

Dispositivos móviles y teletrabajo

Dispositivos móviles

Se trata de disponer de políticas de Seguridad de la Información como medidas concretas que mitiguen los riesgos de la seguridad de la información en el uso de dispositivos móviles o remotos en una organización.

La política de uso de dispositivos móviles en una organización debe considerar:

- El registro de nuevos dispositivos. La cancelación de registro de dispositivos móviles. Requisitos de seguridad física.
- Requisitos de seguridad técnica incluidas conexiones remotas.
- Control de software.
- Control de acceso y cifrado de la información contenida en reposo y en tránsito.

Las políticas diseñadas para dispositivos móviles además de los requisitos anteriores deberían considerar las condiciones de uso de dispositivos móviles y cuando sean apropiados.

Un tema especial a tener en cuenta será el de los dispositivos personales de los propios empleados que utilizan para el trabajo (BYOD). Para ello será necesario determinar si se permiten o no, y en caso afirmativo, determinar en la política cómo gestionarlos (p.e. tratarlos como un dispositivo adicional de la organización e incluirlo en las herramientas de gestión móvil creando en los dispositivos dos perfiles, uno personal y otro de trabajo, en el cual se cifre la información como agenda, correos electrónicos, información descargada, etc).

Teletrabajo

En la actualidad, el teletrabajo es una actividad relativamente difundida en todo tipo de organizaciones, por lo que la seguridad de la Información es un aspecto clave para garantizar la protección de esta actividad. Se trata de:

- Evaluar que activos de información están involucrados en el teletrabajo.
- Realizar una evaluación de riesgos aplicada a los activos de la información y a las actividades del teletrabajo.
- Aplicar los controles adecuados para mitigar los riesgos identificados.

Restricciones o controles para las actividades de teletrabajo según la norma ISO 27002:

- La seguridad física existente del sitio de teletrabajo, considerando la seguridad física del edificio y del entorno local.
- El entorno físico de teletrabajo propuesto.
- Los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a ser accedida y pasada sobre el enlace de comunicación y la sensibilidad del sistema interno.
- La provisión de acceso al escritorio virtual que impide el procesamiento y el almacenamiento de información sobre el equipo de propiedad privada.
- La amenaza de acceso no autorizado a la información o a los recursos de otras personas que utilizan el alojamiento, por ejemplo, familiares y amigos.
- El uso de redes domésticas y requisitos o restricciones de la configuración de los servicios de red inalámbricos.
- Las políticas y los procedimientos para evitar conflictos relativos a los derechos de propiedad intelectual desarrollados en los equipos de propiedad privada.
- El acceso a los equipos de propiedad privada (para verificar la seguridad de la máquina durante la investigación), que puede ser prevenido por la legislación.
- Los acuerdos de licencia de licencia software en los que las organizaciones pueden ser responsables de la concesión de licencias a los clientes de software en estaciones de trabajo de propiedad privada.
- La protección ante software malicioso y los requisitos de firewall.

La norma nos propone además una lista de aspectos a considerar en la definición de las normas o reglas de aplicación del teletrabajo:

- El suministro de equipo adecuado y mobiliario de almacenamiento para las actividades de teletrabajo, donde no se permite el uso de equipo de propiedad privada, que no se encuentra bajo control de la organización.
- Una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede tratar y los sistemas y servicios internos a los que el teletrabajador se encuentra autorizado a acceder.
- El suministro de equipo adecuado de comunicación, incluyendo los métodos para asegurar el acceso remoto.
- La seguridad física.
- Las reglas y directrices del acceso de la familia y visitas al equipo y la información.
- El suministro de soporte y mantenimiento de hardware y software.
- La provisión de seguros.
- Los procedimientos para el respaldo y la continuidad del negocio.
- La auditoría y el control de la seguridad.
- La revocación de la autorización y de los derechos de acceso, y el regreso de los equipos cuando las actividades de teletrabajo finalizan.

Gestión de activos

Los inventarios de activos son un elemento clave para la identificación del riesgo. Solo así podremos establecer las amenazas y vulnerabilidades reales a las que está expuesto el sistema.

Otra razón de gran importancia, es que, gracias al registro del inventario de activos podemos identificar quién es el propietario del activo y asignar responsabilidades. De esta forma, logramos proteger la confidencialidad, la integridad y la disponibilidad (y otras dimensiones que puedan ser necesarias) de la información.

El objetivo de estos controles es la preservación de los activos de información como soporte del negocio. Se focaliza en varias vertientes:

- Responsabilidad de los activos: EL objetivo de este punto es la identificación de los activos de información y las responsabilidades sobre los mismos, con el objetivo de evaluar las medidas de protección adecuadas para cada activo en base a una evaluación de riesgos.
- Clasificación de la información: Asegurar que la información recibe el nivel de protección adecuado de acuerdo con su importancia en la organización.
- Manejo de los soportes de almacenamiento: Se trata de proteger la información en el nivel de soportes en los que se encuentra ya sea papel o soportes electrónicos. Prevenir la exposición, modificación, eliminación o destrucción de información almacenada en medios de forma no autorizada.

Responsabilidad de los activos:

- Inventario de activos: Los activos asociados con la información y las instalaciones de procesamiento de la información deberán ser identificados, y un inventario de los mismos creado y mantenido. La organización debería identificar los activos relevantes en el ciclo de vida de la organización y documentar su importancia. Este inventario deberá ser exacto, actualizado, consistente y alineado con otros inventarios. Por cada ítem identificado, al menos el propietario del mismo y su nivel de clasificación deberán ser consignados.
- Propiedad de los activos: Los individuos así como las entidades que tengan responsabilidades de gestión aprobadas para el ciclo de vida de los activos cualifican como responsables de dichos activos. Se debe implementar un proceso para asegurar la asignación en tiempo de la propiedad de los activos. Esta propiedad debería ser asignada tras la creación de los activos o tras su transferencia a la organización. El propietario será responsable por la correcta gestión de sus activos durante todo el ciclo de vida de estos, como asegurar que están inventariados, clasificados y protegidos, definir y revisar periódicamente los permisos de acceso correspondientes, o asegurar su manejo correcto cuando sean destruidos o borrados.
- Uso aceptable de los activos: Se deben identificar, documentar e implementar las reglas para el uso correcto de la información y de los activos asociados con la información así como de las instalaciones de procesamiento.

- Devolución de activos: Todos los usuarios, tanto internos como externos, deberán devolver todos los activos organizacionales que se les asignaron para su trabajo tras finalizar su empleo, contrato o acuerdo. El proceso de terminación debería estar formalizado para incluir la devolución de todos los activos, físicos y digitales, propiedad de la empresa o que han sido encomendados a la misma. En el caso de que se estén utilizando medios propios, se deberá asegurar que toda la información contenida en los mismos es borrada.

Clasificación de la información:

- Clasificación de la información: La información debería ser clasificada en base a sus requisitos, valor, criticidad y sensibilidad a modificación o exposición no autorizados. Las clasificaciones y los controles de seguridad asociados deberán tener en cuenta las necesidades de negocio para compartir o restringir la información, así como los requisitos legales. Los activos no de información pueden ser clasificados en base a la información que tratan (almacenan, transmiten, procesan, etc). Los propietarios son los responsables por la clasificación de cada activo. El esquema de clasificación debería contener convenciones para la clasificación y el criterio para su revisión regular. El nivel de protección de los activos debería ser evaluado mediante el análisis de la confidencialidad, integridad y disponibilidad, así como otros requisitos de la información considerada. Este esquema así mismo debería estar alineado con la política de control de acceso.
- Etiquetado de la información: Se debe crear un conjunto de procedimientos para el etiquetado de la información de acuerdo al esquema de clasificación establecido por la organización y cubriendo la información en papel y en formato digital. Las etiquetas deberían ser fácilmente reconocibles y estar alineadas con el esquema de clasificación de la organización.
- Manejo de los activos: Se deben desarrollar e implementar procedimientos para la gestión de activos de acuerdo a su nivel de clasificación, incluyendo gestión, procesamiento, almacenamiento, y comunicación de la información, considerando aspectos como:
    - Restricción de accesos que soporten los requisitos de protección de cada nivel de clasificación.
    - Mantenimiento de un registro formal de los recipientes de activos autorizados.
    - Protección de las copias temporales y permanentes de la información a un nivel consistente con la protección requerida en el original.
    - Almacenamiento de los activos TI de acuerdo a las especificaciones de los fabricantes.
    - Marcado claro de todas las copias de los medios para la atención de los recipientes autorizados.

Manejo de los soportes de almacenamiento:

- Gestión de soportes extraíbles: Los soportes extraíbles pueden suponer una brecha importante en la seguridad de la información, por lo que se deben tener en cuenta aspectos como:
    - La necesidad de su uso.
    - Los soportes reutilizables que deberían retirarse de la organización y hacerse irrecuperables.
    - Requerir autorización para su uso cuando sea factible.
    - Mantener un registro de altas y bajas
    - Considerar especificaciones de almacenamiento según especificaciones del fabricante.
    - Cifrar datos para proteger aquellos que se consideren importantes (confidencialidad e integridad).
    - Renovar dispositivos con un periodo determinado para evitar la degradación de datos necesarios e importantes.
    - Proteger la información almacenada con copias de seguridad en soportes independientes.
    - Crear un registro de soportes extraíbles para limitar la posibilidad de pérdida de datos.
    - Controlar la transferencia de información hacia medios extraíbles.
    - Documentar los procedimientos de autorización.
- Eliminación de soportes: Se deben establecer procedimientos para la eliminación segura de soportes a la finalización de su uso. Se trata de minimizar o evitar que los datos sensibles o confidenciales puedan ser recuperados una vez que el dispositivo se da de baja mediante procedimientos de eliminación segura, teniendo en cuenta aspectos como:
    - Establecer un proceso de eliminación segura de datos que no permita su recuperación.
    - Identificar que dispositivos requieren de un proceso de eliminación segura.
    - Controlar la utilización de empresas externas para la realización de tareas de eliminación segura estableciendo algún tipo de control.
    - Mantener un registro dispositivos que han sido dados de baja de forma segura por contener información sensible.
- Traslado de soportes físicos: Se debe desarrollar e implementar un proceso para proteger la información cuando los soportes necesitan ser trasladados entre distintas ubicaciones, teniendo en cuenta aspectos como:
    - El registro de salida de los soportes para su cotejamiento con el transportista y el lugar de destino de mismo incluyendo un control de tiempos de transporte.
    - Control de transportistas (Utilizar transportistas de confianza).
    - Mantener una lista de transportistas autorizados.
    - Controlar la identificación del transportista o mensajero.
    - Establecer un procedimiento de cifrado cuando sea necesario y posible.
    - Controlar los embalajes y las condiciones ambientales (humedad, temperatura, polvo etc.) con las especificaciones del fabricante.

Seguridad en RRHH

El objetivo del presente dominio es la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.

Es necesario reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

Se requiere explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información y se encuentren capacitados para respaldar la Política de Seguridad de la organización en el transcurso de sus tareas normales es esencial y se considera la una de las barreras de seguridad y de protección esenciales en cualquier organización.

Antes de la contratación

El objetivo es asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen y con ellos reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

Los siguientes controles deben estar implementados:

- Investigación de antecedentes: Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
- Términos y condiciones de contratación: Como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.

Durante el contrato

El objetivo es asegurar que los empleados y contratistas conocen y cumplen con sus responsabilidades en materia de seguridad de la información.

Los siguientes controles deben estar implementados:

- Responsabilidades de gestión: La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos.
- Concienciación, educación y capacitación en SI: Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros, deberían recibir formación apropiada y actualizaciones regulares en políticas y procedimientos organizacionales que sean relevantes para la función de su trabajo.
- Proceso disciplinario: Debería existir un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad. Esto puede ser complicado en determinados países con una ley muy garantista con los trabajadores, pero en todo caso, y acomodándose siempre a lo que estipule la ley, se debe crear un procedimiento disciplinario.

Tras la finalización del contrato o cambio de puesto

El objetivo es el de proteger los intereses de la organización durante el proceso de cambio o finalización de empleo por parte de empleados y contratistas.

Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente. Por ejemplo, en caso de terminación de un puesto por despido o cese del contrato con una tercera parte, se deberían revocar los permisos de acceso previo a la comunicación (para evitar posibles vendetas).

Controles de mitigación: Seguridad física

La seguridad física es la disciplina que diseña, despliega y mantiene controles de seguridad aplicables al mundo físico con el objeto de proteger diferentes tipos de activos:

- Áreas y espacios.
- Equipamiento.
- Personas.

Si bien las personas son el bien más valioso. y el fin último de la seguridad en las organizaciones, generalmente las medidas para proteger a las mismas está incluidas en las otras dos (especialmente la protección de áreas y espacios).

A continuación se listan los controles específicos para crear y mantener áreas seguras:

- Perímetro de seguridad física: Control orientado a proveer protección contra la entrada no autorizada.
  - Seguridad perimetral: Los requisitos para la seguridad física deben tener en cuenta los niveles de protección del perímetro de las instalaciones o elementos que contienen la información a proteger con controles como muros, vallas, alarmas, protección de ventanas, cerraduras, etc.
  - Áreas atendidas: las áreas restringidas a personal autorizado deberían contar con un área de recepción atendida o medios de control adecuados para limitar el acceso físico.
  - Barreras: Si es aplicable deberían considerarse barreras físicas que impidan el acceso no autorizado y protejan el área de agentes ambientales adversos.
  - Sistemas Anti-incendios: Contar con sistemas de protección contra el fuego cumpliendo con la legislación vigente.
  - Detección de intrusión: Se deben considerar sistemas de detección de intrusos (p ej. Alarmas).
  - Segmentación de espacios: Deberían separarse físicamente las áreas de proceso de información que van a ser gestionadas por personal externo de las propias de la organización.
- Controles de acceso físico: Aquellas áreas que se consideran seguras deben estar protegidas por controles de entrada que permitan solo personal autorizado incluyendo la asignación, modificación y eliminación de los permisos de acceso, sistemas de entrada como tornos, monitorización de los diferentes punto de entradas (sensores de movimiento, cámaras de vigilancia, etc), registro y análisis de las entradas y salidas (tanto personal interno como externo y visitas) gestión del personal externo, uso de identificadores (como tarjetas), etc.
- Seguridad de oficinas, despachos e instalaciones: Las instalaciones deben diseñarse para evitar al máximo posible el riesgo que la información confidencial sea accesible para los visitantes. Para ello se debe evitar siempre que sea posible que las áreas claves estén en sitios con paso público, evitar carteles y otros signos que aporten demasiada información sobre el edificio y las áreas internas, que la información y las actividades realizadas en áreas sensibles puedan ser visibles/audibles desde fuera, etc.
- Protección contra amenazas externas y medioambientales: Se deben diseñar controles contra desastres naturales, ataques maliciosos y accidentes (como inundaciones, fuego, terremotos, explosiones, ataques terroristas, manifestaciones públicas, etc).
- Trabajo en áreas seguras: Se deben diseñar e implementar procesos para el trabajo en áreas seguras, teniendo en cuenta aspectos como que el personal sólo debería saber de la existencia de, y los trabajos realizados en, áreas seguras según el criterio de necesidad de saber, evitar el trabajo no supervisado en áreas seguras, las áreas seguras vacías deberían quedar cerradas y protegidas o evitar cualquier tipo de grabación en estas áreas.
- Áreas de entrega y carga: Los puntos de carga y de entrega de mercancía suelen ser puntos sensibles para la seguridad física por lo se debería tomar en cuenta algunos aspectos como horarios definidos de apertura y cierre, control de apertura y cierre de puertas externas e internas, control de personal, realización de inventarios de materiales entregados, revisión de mercancías entregadas para detectar materiales peligrosos o separar entregas entrantes y salientes o barreras adicionales de seguridad.

Así mismo, es primordial asegurar que se proteja el equipamiento:

- Ubicación y protección del equipamiento: Se debe proteger el equipamiento de la organización dado que en el mismos e realiza el procesamiento y/o almacenamiento de la información, teniendo en cuenta controles como:
  - Colocación del equipamiento para minimizar el acceso innecesario a las áreas de trabajo.
  - Colocación de las áreas de procesamiento de información donde se gestione información sensible de forma que se minimice el riesgo de escuchas o vistas de dicha información.
  - Las instalaciones de almacenamiento estarán protegidas contra acceso indebido.
  - Los ítems que requieran de un mayor nivel de protección deberán ser protegidos especialmente y en áreas específicas para reducir el nivel general de protección necesario.
  - Se deben implantar controles para evitar daños al equipamiento como fuego, humo, sobrecargas eléctricas, agua, polvo, químicos, etc.
  - Se deben crear y mantener guías para comer, beber y fumar cerca del equipamiento para evitar su daño.
  - Se deben monitorizar las condiciones ambientales como humedad y temperatura para asegurar que están dentro de los límites seguros para el equipamiento.
  - Se debe aplicar protección contra electricidad en los edificios y desplegar filtros de protección de electricidad en todas las líneas eléctricas y de comunicaciones.
  - El equipamiento que maneje información sensible deberá estar protegido contra fugas electromagnéticas.
- Elementos de soporte: El equipamiento será protegido contra fallos en el suministro eléctrico y otras disrupciones causadas por los elementos de soporte (electricidad, comunicaciones, agua, gas, alcantarillado, etc).

- Seguridad en el cableado: Todo el cableado de comunicaciones y suministro de electricidad será protegido contra intercepción, interferencias o daño. Se deberán tener en cuenta como el enterramiento o protección adecuada de los cables, segregación de cables de comunicación y electricidad para evitar interferencias y para cableado de sistemas críticos aspectos como el uso de conductos blindados y puntos de acceso protegidos, uso de apantallado electromagnético, acceso controlado a las salas de cableado o paneles de acceso, etc.
- Mantenimiento del equipamiento: El equipamiento deberá ser mantenido siguiendo todas las indicaciones de los fabricantes con el fin de optimizar su vida útil y evitar fallos en la integridad y disponibilidad de la información.
- Retirada de bienes: El equipamiento, información y software no será retirado sin la correspondiente autorización y asegurando que quede un registro de la salida y entrada de los mismos.
- Seguridad del equipamiento y de los activos fuera de las instalaciones: Se deben proteger los activos fuera de la organización tomando en cuenta los diferentes riesgos externos, teniendo en cuenta aspectos como dejar ningún equipamiento desatendido, tener elementos específicos de protección como cables y candados, etc.
- Seguridad en la reutilización o eliminación de equipos: Todos los equipos que contengan medios de almacenamiento deberán ser verificados para asegurar que todos los datos sensibles y el software licenciado han sido eliminados so sobrescritos de forma segura antes de su eliminación u reutilización (puede ser tanto destrucción física como cifrado, reescritura segura, uso de medios de des-magnetizado, etc).
- Equipamiento desatendido por el usuario: Los usuarios no deben dejar las sesiones abiertas mientras el equipo no este atendido. Además de los procedimientos de bloqueo de pantalla, la sesión de la aplicación y de la red debe cerrarse cuando las conexiones no se utilizan. Esto debería aplicarse tanto a los dispositivos móviles como a los equipos fijos.

Controles de mitigación: Seguridad Lógica

Gestión de la identidad y el control de acceso

La gestión de identidades y accesos, es un término genérico para los procesos internos de una organización que se enfocan en administrar cuentas de usuario y recursos de red corporativa, incluidos los derechos de acceso para las organizaciones, usuarios, aplicaciones y sistemas.

Junto a estos procesos, podemos encontrar una disciplina dentro del software que busca crear productos para automatizar estos procesos y hacerlos más efectivos y homogéneos.

Terminología de Gestión de Identidades y Control de Accesos:

- Gestión de accesos: El proceso de configurar el nivel de acceso para cada usuario y grupo dentro de un sistema. A través de este proceso, los administradores, conceden acceso a usuarios autorizados y restringen el acceso a los usuarios no autorizados. Esto se puede realizar de forma jerárquica a través del uso de grupos de usuarios. La gestión de accesos requiere de auditoria periódica y mantenimiento para mantenerse al día con el negocio en continua evolución y los roles de los empleados.
- Necesidad de saber / Menor privilegio: Se trata de dos principios que regulan las buenas prácticas de la gestión de accesos y la provisión de permisos. El primero regula que los usuarios sólo deberían tener acceso a aquella información que sea imprescindible para realizar su trabajo y a nada más. El segundo dice que los usuarios deberían tener los privilegios mínimos que les permitan realizar su trabajo.
- Aprovisionamiento / Desaprovisionamiento: El primero es el proceso de establecer una identidad y su acceso asociado en un sistema. El segundo es el proceso de eliminar dicho acceso y las identidades asociadas cuando un usuario se va, es despedido, cambia de área o puesto (y por tanto requiere de nuevos accesos y permisos) o su contrato finaliza.
- Identificación, autenticación y autorización: Estos términos son la triada del control de acceso, mostrando el flujo en el que un usuario accede a un sistema. LA identificación es el proceso por el que un usuario establece cual es su identidad. La autenticación es el proceso por el cual el sistema verifica de alguna manera que el usuario tiene realmente la identidad proclamada (que nadie le esté usurpando). Y por fin, la autorización, es una vez identificado y autenticado al usuario, el sistema comprueba los permisos de acceso que tiene a dicho sistema.
- Factores de Autenticación / 2FA / MFA: Existen diferentes esquemas de autenticación de usuarios, basados en la propiedad del factor utilizado para verificar la identidad. El primero es “algo que sabes”, basado generalmente en el uso de un usuario y contraseña. El Segundo factor es “algo que tienes” o autenticación biométrica, en el que el Sistema comprueba alguna característica física del usuario como su huella digital, el iris, la palma de la mano, su huella de voz, etc. Finalmente “algo que tienes”, en el cual la autenticación se basa en la posesión de un objeto como una smartcard, token que genera contraseñas aleatorias de forma temporal o smartphone al que llegan contraseñas temporales. Para mejorar la seguridad del acceso, se recomienda, al menos para sistemas críticos, el uso de más de un factor de autenticación (2FA o doble factor de autenticación o MFA o multifactor de autenticación).
- Acceso basado en roles (RBAC): Se trata de un paradigma de gestión del acceso y el privilegio en el cual se definen roles empresariales de acceso a los cuales se les conceden acceso a diferentes sistemas (cada uno de ellos con un conjunto de permisos). Así, a cada usuario, de acuerdo a su puesto de trabajo se le asignarán uno o más roles. Este modelo es el más utilizado actualmente, si bien existen otros modelos como el Control de Acceso discrecional o DAC (método de restricción de acceso a objetos que se basa en la identidad de los sujetos que pretenden operar o acceder sobre ellos, es decir, se concede a cada individuo un conjunto de permisos personalizado) y el Control de Acceso Obligatorio o MAC (Este mecanismo de acceso es complementario y añade una capa adicional. Se basa en un “etiquetado” de todo elemento del sistema y sobre las cuales se aplicarán las políticas de control de acceso configuradas. Así, cualquier operación de un sujeto sobre un objeto será comprobado las etiquetas y aplicando las políticas MAC establecidas para determinar si la operación está permitida, aún incluso cuando se hayan cumplido otros controles de seguridad. Este sistema viene de sistemas militares y aún se aplica a sistemas gubernamentales, de inteligencia, etc).
- Flujos de trabajo Altas, Bajas y Modificaciones: Cada vez que se quiere aprovisionar (alta), desaprovisionar (baja) o modificar los permisos o rol de un usuario, se debe contar con un flujo de trabajo en el que los roles involucrados y los pasos a dar estén claramente definidos. Quién puede solicitarlo, quién/es debe/n aprobarlo, quién lo audita/monitoriza, etc.
- Inicio de Sesión Único (SSO): Se trata de un mecanismo de control de acceso que permite que un usuario se autentique una vez ante un sistema maestro y este gestione sus credenciales contra otros sistemas de forma que no sea necesario volverse a autenticar (generalmente durante un periodo definido o bien hasta el cierre de sesión).
- Contraseña de un solo uso (OTP): Mecanismo de acceso basado en una contraseña es válida una sólo vez. Esto puede ser mediante sistemas que generan contraseñas de forma aleatoria y regular en el tiempo (cliente y servidor la misma contraseña) o bien mediante el envío de la contraseña a un dispositivo de usuario como teléfono (bien por SMS o más seguro, disponiendo de una aplicación desplegada).

Requisitos del negocio para el control de accesos:

- Política de control de acceso: Una política de control de acceso debe ser establecida, documentada y revisada basada en los requisitos de seguridad del negocio y de la información. Los propietarios de los activos deberán determinar las reglas de control de acceso apropiadas, los derechos de acceso y restricciones para determinados roles de usuarios, con el nivel de detalle y de dureza de los controles que reflejen los riesgos de seguridad asociados. Los controles de acceso pueden tanto físicos como lógicos y se deberían considerar en conjunto. Tanto a los usuarios como a los proveedores de servicios se les debería dar una declaración clara de los requisitos de negocio que los controles deben alcanzar. La política debería tener en cuenta los siguientes aspectos:
    - Requisitos de seguridad para las aplicaciones de negocio.
    - Políticas para la diseminación de la información y autorización (p.e la necesidad de saber y los niveles de seguridad y clasificación de la información).
    - La consistencia entre los derechos de acceso y las políticas de clasificación de la información de sistemas y redes.
    - La legislación relevante y cualquier obligación contractual respecto de la limitación de acceso a datos o servicios.
    - La gestión de derechos de acceso en un entorno distribuido y en red que reconozca todos los tipos de conexiones existentes.
    - Segregación de los roles de control de acceso (p.e petición de acceso, autorización, administración del acceso, etc).
    - Requisitos para la autorización formal de las peticiones de acceso.

    - Requisitos para la revisión periódica de los derechos de acceso.
    - Eliminación de los derechos de acceso.
    - Archivado de los registros de todos los eventos significativos relacionados con el uso y gestión de las identidades de usuario y la información secreta de autenticación.
    - Roles con acceso privilegiado.
- Acceso a las redes y a los servicios de red: Se trata de un requisito para la gestionar la autorización de los usuarios que acceden a los recursos de red. Para ello se exige como requisito elaborar una política específica para el uso de los recursos de red. Aunque este está cubierto en gran parte por el anterior, la política de "gestión de acceso de usuarios de red" debe determinar a qué información se puede acceder, los procedimientos de autorización, los controles de gestión para la protección de las redes, las conexiones de red permitidas (p. Ej., No mediante wifi), los requisitos de autenticación y la supervisión del uso. La política debe identificar:
    - La red y servicios a los cuales se accede.
    - Los procedimientos de autorización.
    - Que controles tienen estos procedimientos.
    - Los medios por los cuales se accede (VPN, Wifi etc.).
    - Los requisitos de autenticación.
    - Como se supervisa (monitorización) el uso de los servicios de red.

Gestión del acceso de usuarios:

- Registro de usuarios y cancelación del registro: Se trata de un control para el alta y baja de los usuarios. Este control exige establecer un proceso de altas y bajas que permite los derechos de acceso teniendo en cuenta:
    - Un registro de IDs o cuentas de usuario donde se vincula o identifica al usuario.
    - Los IDs deben desactivarse automáticamente o de forma inmediata cuando el usuario abandona la organización.
    - Eliminación periódica de usuarios redundantes.
    - Los IDs redundantes nunca pueden ser asignados a otros usuarios.
    - El proceso de cancelación debería tener en cuenta:
        - La revocación del ID del usuario.
        - La revocación de los permisos del ID de usuario.
- Gestión de acceso a los usuarios: Se debe establecer un proceso formal para asignar y revocar los accesos a sistemas y servicios que:
    - Incluya la aprobación del propietario del servicio o sistema.
    - Verifique si el acceso cumple con las políticas de acceso definidas.
    - Se garantice que el acceso no se da hasta finalizar el proceso de autorización.
    - Asegure que se mantiene un registro de los accesos concedidos.
    - Asegure que se eliminan los accesos de usuarios que han abandonado la organización.
    - Asegure que se modifican los accesos de usuarios que han cambiado de función o puesto de trabajo si proceda.
    - Asegure que se revisan periódicamente los derechos de acceso.
- Gestión de derechos de acceso privilegiados: El control de los derechos de acceso privilegiados debe realizarse de forma independiente mediante un proceso específico que:
    - Tenga en cuenta las políticas de acceso privilegiado definidas.
    - Se identifiquen accesos privilegiados de cada sistema o proceso.
    - Se tenga en cuenta las reglas generales de mínimos privilegios.
    - Se establezca una norma de caducidad de los permisos privilegiados.
    - Se definan IDs especiales o distintos para las cuentas de uso normales o no privilegiadas.
    - Se definan procedimientos para evitar el uso no autorizado de cuentas con derechos de acceso privilegiados.
    - Se verifiquen periódicamente las competencias de los usuarios.
    - Considere mecanismos para mantener la confidencialidad de los datos de acceso de usuarios genéricos para los usuarios privilegiados o mecanismos para forzar el cambio de contraseñas cuando un usuario privilegiado abandona o cambia de puesto de trabajo.
- Gestión de la información de autenticación secreta de los usuarios: Control para garantizar que se mantiene la confidencialidad de la información secreta de acceso (p. ejemplo contraseñas, tokens, smartcards, etc). Gestionar la información de autenticación supone controlar:
    - Incluir cláusulas en contratos y condiciones de puesto de trabajo sobre el mantenimiento del secreto de las contraseñas o información de autenticación.
    - Obligación de cambiar contraseñas iniciales después de su primer uso.
    - Identificar al usuario antes de entregar las contraseñas y obtener acuse de recibo.
    - Uso de contraseñas seguras, no compartidas.
    - Uso de medios seguros de comunicación (Correos cifrados etc.).
    - Cambiar contraseñas a personal externo después de que han realizado sus trabajos (instalaciones de software etc.).
- Revisión de derechos de acceso de usuario: Control para establecer una revisión periódica de los permisos de accesos de los usuarios que tenga en cuenta aspectos como:
    - Revisar derechos de acceso a la terminación de empleo o cambios en la organización (cambios de empleo o promociones).
    - Limitar en el tiempo los derechos de acceso con privilegios especiales.
    - Revisar las cuentas con privilegios especiales periódicamente y registrar los cambios que se realicen.
- Eliminación o ajuste de los derechos de acceso: Control para garantizar que se modifican los derechos de acceso al finalizar el empleo o cambiar de puesto de trabajo dentro de la organización.

Para realizar esto, además de políticas y procedimientos, se debería implantar por cada aplicación un concepto de autorización. este documento contiene información sobre:

- Proceso de petición de nuevos usuarios o modificación de los existentes (mediante correo electrónico, herramienta de ticketing, etc).
- Proceso de aprobación para el alta, baja y modificación de usuarios (con roles y responsabilidades, pasos, etc).
- Listado de roles y permisos de acceso para la aplicación (incluyendo a nivel de infraestructura y de aplicación. si bien la infraestructura, si se gestiona de manera medianamente centralizada pueden tener su propio concepto de autorización propio y central) .
- Proceso de revisión de los roles y permisos (quién, cómo, cuando, etc. El proceso puede tener tiempos diferentes para usuarios regulares y privilegiados).

Responsabilidades del usuario:

Uso de la información de autenticación secreta: Cada organización debe establecer normas para la utilización de contraseñas teniendo en cuenta aspectos como:

- Asegurar que las contraseñas no se divulguen.
- Evitar el uso de registros de contraseñas (papel, archivos etc.).
- Políticas para cambiar las contraseñas ante amenazas.
- Políticas para la calidad de las contraseñas, teniendo en cuenta aspectos como:
    - Tamaño (Menos de 10 caracteres se consideran triviales hoy en día, y eso si se cumplen las reglas de complejidad).

    - Complejidad (regla 3 de 4, utilizar al menos un carácter de tres grupos de entre 4 posibles, minúsculas, mayúsculas, numéricos y caracteres especiales como @¿?.
    - Validez temporal (cambiarla cada cuánto tiempo).
    - Se deberán tener criterios más o menos estrictos dependiendo de si la cuenta es de usuario normal, servicio, privilegiada, compartida, etc.
- Evitar el almacenamiento de contraseñas.
- Forzar cambios de contraseñas iniciales.
- Evitar compartir contraseñas para distintos usos.

Control de acceso a sistemas y aplicaciones:

- Restricción de acceso a la información: Las funciones de una aplicación o sistema deben considerar las restricciones de control de acceso determinadas por la política de control definido. Se deben tener en cuenta aspectos como:
    - Utilizar menús para controlar el acceso a las distintas funciones.
    - Ocultar las funciones de administración a los usuarios habituales.
    - Determinar que datos son accesibles determinando que datos pueden estar disponibles para cada ID de usuario.
    - Restringir de forma selectiva derechos de lectura / escritura / eliminación / ejecución etc.
    - Limitar el tipo de información de salida.
    - Considerar accesos físicos o lógicos adicionales para sistemas o información altamente clasificados.
- Procedimientos de conexión (log-on) seguros: Donde se requiera por la política de control de accesos, el acceso a los sistemas y aplicaciones debería estar controlado por un proceso de acceso (log-on) seguro. El nivel de rigor para establecer la identidad del usuario dependerá de la criticidad del sistema y la información gestionada. Puede ser desde 1 factor de autenticación a un doble factor con usuario y contraseña y una smartcard o aplicación en el móvil. El método de acceso debe mostrar la información mínima sobe el sistema o aplicación para evitar ofrecer a un usuario no autorizado información que podría ayudar en un ataque. En general se deben tener en cuenta aspectos como no mostrar identificadores hasta haber pasado el proceso exitósamente, no mostrar mensajes de ayuda, validar la información sólo cuando esta esté completa, y en caso de error, no mostrar donde ocurrió este, proteger contra intentos de fuerza bruta, generar eventos de los intentos exitosos y fallidos de acceso, no mostrar las contraseñas en claro ni enviarlas sin cifrar por la red, etc.
- Sistema de gestión de contraseñas: Se debe automatizar en los sistemas y aplicaciones, cuando esto sea técnicamente posible, la seguridad de las contraseñas, filtrando aquellas que no cumplan los requisitos establecidos. Un sistema así debe tener en cuenta aspectos como:
    - Reforzar el uso de IDs individuales así como contraseñas para mantener la responsabilidad individual (accountability).
    - Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para permitir errores de entrada.
    - Reforzar la selección de contraseñas de calidad.
    - Forzar a los usuarios a cambiar sus contraseñas cuando entren por primera vez.
    - Forzar el cambio regular de contraseñas y cuando sea necesario (p.e sospecha de intrusion en la cuenta).
    - Mantener un registro de las contraseñas utilizadas y prevenir su re-uso.
    - No mostrar contraseñas en la pantalla mientras se entran.
    - Almacenar los ficheros de contraseñas separados de los datos de la aplicación.
    - Almacenar y transmitir las contraseñas de forma protegida (p.e cifradas).
- Uso de programas de utilidad privilegiados: Aquellos programas con capacidades de anulación del sistema o sus controles deben ser restringidos y supervisados de manera especial. Los programas con funciones privilegiadas deberían requerir autenticación por separado y estar segregados de las aplicaciones del sistema. Todas las actividades realizadas deben registrarse. Se debe considerar nuevamente la segregación de funciones cuando sea posible.
- Control de acceso al código fuente de programas: El acceso al código fuente y elementos asociados (como diagramas, diseños, especificaciones, etc) deberá ser estrictamente controlado para evitar cambios no controlados y el acceso a partes sensibles que podrían dar a un potencial atacante una ventaja.

Aplicaciones de gestión de identidades y control de acceso

La gestión de la identidad y del acceso, frecuentemente conocida por su acrónimo anglosajón IAM (por “Identity and Access Management”) es un área de negocio que se dedica a las siguientes tareas:

- Aprovisionamiento de cuentas de usuario y contraseñas, mediante automatismos, de acuerdo con políticas bien definidas y aplicadas.
- Implantación de sistemas de identificación y autenticación única corporativa (también denominado “single sign-on”).
- Gestión centralizada de las atribuciones de los usuarios, basada en directorios de usuarios (habitualmente basados en LDAP).
- Modelo de autorizaciones, que concentra en un solo punto las autorizaciones de acceso.

La necesidad de negocio que cubre la gestión de identidad es facilitar y controlar de forma eficiente los sistemas de identificación y autenticación, autorización y auditoria (AAA) que emplean las organizaciones en sus procesos basados en tecnologías de la información. Entre los beneficios perseguidos destacan los siguientes:

- Seguridad: La automatización y la gestión centralizada permite a las organizaciones alinear el acceso con las funciones de trabajo, asegurar que las políticas de seguridad son aplicadas consistentemente, y mejorar la fiabilidad de los procesos de seguridad.
- Eficiencia: El auto-servicio, la automatización y la visibilidad de la asignación de recursos reduce el coste de la organización dentro y fuera de TI.
- Simplicidad: La capacidad de Single sign-on (SSO) y las identidades federadas (el uso de sistemas IAM entre diferentes organizaciones que confian el uno en el otro para delegar la autenticación cuando un agente de una organización accede a la otra) reducen la frustración de los usuarios y mejora el uso de las aplicaciones clave.
- Productividad: La automatización, el uso de worflows y el auto-servicio permiten procesos más eficientes, proveyendo tiempos de respuestá más rápidos y permitiendo al personal centrarse en tareas de alto valor.
- Cumplimiento: La centralización y la automatización permiten revisiones de auditoría automatizadas, mejorar el seguimiento de la actividad de usuario y la certificación de acceso de cara al cumplimiento, y aportar mayor confianza en el proceso IAM.

Un proyecto típico de diseño de una solución IAM sigue los siguientes pasos:

1. Crear una visión de arquitectura: El proyecto de despliegue debe llevarse a cabo en el contexto de una visión general de Gestión de Identidad y Accesos. Cada proyecto de IAM no sólo debe proporcionar un valor medible sino también mover a la organización más cerca de las metas generales de IAM. Por lo tanto, el primer paso es crear una visión de la arquitectura para sus capacidades de IAM, incluyendo componentes a corto, medio y largo plazo. Esta visión de la arquitectura servirá como una guía para las decisiones a tomar. Por ejemplo, una visión IDaaS de gestión de identidad, primeramente guiaría a la organización a una estrategia de despliegue cloud, donde es probable que tengamos que incluir un soporte robusto para las actuales y futuras aplicaciones SaaS.
    - Involucrar al negocio de forma temprana: Al considerar una visión de la arquitectura a largo plazo de la gestión de identidad , es crucial involucrar a la parte comercial para entender las metas y objetivos del negocio, anticipándose a las necesidades futuras e identificando nuevas iniciativas comerciales en el proceso de planificación que requieran del apoyo de IAM.
    - Determinar qué usuarios y que dispositivos/aplicaciones se necesitan activar: La definición de funciones de IAM varía según el grupo de usuarios. Por lo tanto, es importante comenzar con un claro entendimiento sobre qué tipos de usuarios o dispositivos/aplicaciones necesitan acceso bajo el alcance de las iniciativas de reinvención de la gestión de la identidad y accesos estamos haciendo.
    - Definir sus funciones de estado futuro por grupo de usuarios: El siguiente paso es identificar las funciones necesarias para dar soporte a cada uno de estos grupos de usuarios / entidades.

    - Realizar un análisis de posibles brechas o casos sin cubrir: Aunque muchas organizaciones son conscientes de los costes, ahorrar dinero se queda en un segundo plano en algunos puntos. En todo caso, no es posible cubrir todo desde el inicio, y estas iniciativas deben seguir ciclos de maduración (a veces de años), y por ello es importante que en cada iteración quede claro lo que no se cubrirá para facilitar el análisis de requisitos en las siguientes iteraciones.
    - Crear una lista de requisitos: Una vez que la organización entiende todas las necesidades que deben ser consideradas, debemos traducir estas necesidades en requisitos para buscar nuestra mejor opción, ya bien sea comercial , open source o similar.
    - Definir cuáles serán las fuentes autoritativas y secundarias de información sobre los usuarios. Uno de los aspectos críticos para un proyecto de este tipo es saber en qué fuentes se puede confiar (autoritativas) para la recolección inicial de usuarios así como para el alta a posteriori (por ejemplo el SAP de RRHH o el DA), y cuales contendrán información adicional útil (secundarias).
2. Crear una hoja de ruta en fases: Es posible que la organización tenga una larga lista de requisitos. Por lo tanto, la priorización y la definición de fases son los pasos clave. Las fases son importantes no sólo porque los presupuestos son siempre finitos, sino porque los proyectos grandes son mucho más difíciles de manejar, teniendo grandes riesgos. Las organizaciones deben administrar su programa IAM como un viaje, no como un destino, estableciendo las expectativas de las iniciativas de IAM que necesitan atención continua.
    - Determinar prioridades por oportunidades de negocio y riesgos: Las prioridades se establecen en función de factores como la eficiencia operacional de IAM y la habilitación del negocios. A veces, las prioridades de IAM son muy obvias. Puede haber un requisito de IAM que esté en la parte superior de la lista en función de la necesidad de apoyar una iniciativa comercial clave o de mitigar un riesgo inaceptable. Algunos ejemplos son la mejora de la experiencia del usuario mediante la consolidación de credenciales de inicio de sesión en todas las líneas de los productos y la satisfacción de los requisitos de cumplimiento. Otras veces se requiere trabajo para descubrir todas las prioridades implícitas.
    - Identificar las piezas IAM que requieren atención inmediata: Antes de que un usuario o entidad pueda acceder a una aplicación, el usuario o la entidad por lo general necesita ser aprovisionado. Y antes de que un usuario pueda ser aprovisionado, la organización necesita crear una identidad para ese usuario o entidad. Esto significa que tener un directorio o una base de datos de usuario apropiada es la primera capa clave de base en IAM. Por lo tanto, uno de los primeros pasos es determinar si un enfoque en directorio es adecuado, si no es así, será difícil optimizar las capas posteriores.
    - Identificar piezas IAM con dependencias: Los módulos de IAM necesitan cada vez más, interoperar con otros módulos de IAM. Muchas funciones de gestión de identidad se están volviendo más inteligentes y, por lo tanto, necesitan comunicarse mucho más profundamente con otros módulos de IAM que antes.
    - Alinear la hoja de ruta con el perfil de riesgo de negocio: Un elemento de la planificación de IAM es la gestión de riesgos. Por lo tanto, las organizaciones deben adoptar un enfoque basado en el riesgo para priorizar los proyectos individuales de gestión de identidad y accesos. La pregunta a hacer es: ¿cuánto se reduce el riesgo por un proyecto de implementación de IAM en particular? Debemos definir el riesgo ámpliamente al realizar este análisis previo.
3. Definir una arquitectura: El enfoque arquitectónico tiene dos componentes: la decisión de hacer o comprar y las opciones de implementación. La primera de ellas es la decisión de comprar o poder reutilizar lo que ya tenemos. No siempre es necesario realizar inversión nueva en software o infraestructura.
    - Determinar el enfoque a crear o comprar: Hay ventajas y desventajas de escribir nuestro propio software IAM desde cero. Las desventajas superan las ventajas. En general, es una buena práctica usar software y servicios de IAM apoyados por un grupo especializado en dar soporte a ese software o servicio. Si no podemos encontrar el software que satisface todas nuestras necesidades, debemos extender el software a nivel de APIs, evitando siempre cambiar el núcleo de la aplicación porque esto puede hacer que el software sea débil y difícil de actualizar.
    - Definir el enfoque a implementación de alto nivel: Las opciones principales son utilizar soluciones comerciales, IDaaS, open-source o homegrown (desarrollado a medida por la organización).
    - Buscar oportunidades de consolidación en grupos de usuarios: Muchos proveedores IAM han añadido características a su oferta inicial de IAM para permitirles soportar múltiples grupos de usuarios en una sola plataforma. Por ello debemos tener en cuenta que estas implementaciones pueden implicar el despliegue de varias instancias para satisfacer las preocupaciones de seguridad y escalabilidad.
    - Validar el enfoque arquitectónico con las necesidades de negocio: El uso de los pasos anteriores para desarrollar un framework preliminar, es sólo el comienzo. A medida que se pasa a un diseño más detallado y la selección de proveedores para cada módulo que se está implementando, tendremos que validar que los recursos necesarios en tiempo de implementación, costo y funcionalidad permanezcan dentro de límites aceptables.
    - Planificación detallada con Quick Wins: Es probable que, a medida que avancemos con la selección preliminar de proveedores para una fase específica, nuestra organización determine que necesitamos hacer compromisos en áreas particulares. O bien seremos nosotros quienes debamos priorizar. Las organizaciones buscan frecuentemente ver pequeños resultados a corto plazo. La gestión de identidad es difícil de extrapolar a beneficios, por lo que deberemos demostrar que los beneficios que la misma nos va aportando, haciendo que el presupuesto apostado en la misma determine beneficios para el negocio.

A continuación veremos los factores críticos de éxito para un proyecto de tal envergadura:

- Se debe asegurar el apoyo total de la dirección y que este continúe durante todo el proyecto para ayudar a mantener el esfuerzo en los límites marcados y reforzar las expectativas. Se debe buscar un campeón del proyecto a alto nivel en el organigrama y atar esta iniciativa al programa de gestión de la identidad global (políticas, procesos, etc). Si no, cuando surjan problemas imprevistos (y surgirán, y muchos) o cuando el propietario de un sistema objetivo crítico decida no limpiar los datos erroneos, no se tendrá el musculo necesario para asegurar el éxito.
- Se deben abrazar las características de la tecnología seleccionada. Si bien no todas las características requeridas estarán presentes y habrá que desarrollar algunos módulos (por ejemplo para la integración con determinados sistemas legacy), la sobre-personalización hará inmantenible el sistema (p.e. da problemas al actualizar la solución base) .
- No se debe hacer mucho demasiado pronto. Se debe asegurar que la solución a construir se mantiene alineada con el roadmap del proyecto y los requisitos previstos. A menudo los stakeholders quieren tratar cada hallazgo de auditoría o los riesgos de un análisis, lo que llevará a un proyecto fallido. Este tipo de proyectos son muy complejos y con líneas temporales de años. Así, se debe evitar intentar implementar todo demasiado pronto (o incluso tener desviaciones de alcance añadiendo al paso nuevas características y requisitos), y seguir un programa de maduración del proceso y la solución. Para ello, el faseado del proyecto (visto anteriormente) facilitará ver un retorno rápido a la vez que mantener el programa de forma estable.
- No se debe sucumbir a la tentación de automatizar procesos malos, tolerar datos incompletos o eliminar requisitos clave. Se debe trabajar con la dirección para restablecer las expectativas, evaluar el riesgo de la iniciativa y desarrollar soluciones alternativas (para eso se debe realizar en fases). Por ejemplo, no se debe llegar al extremo de que no se pueden ejecutar auditorías de cumplimiento (una de las razones de seleccionar una tecnología así) porque los roles o las estructuras de autorización están incompletas.
- Asegurar que se sabe cómo se soportará el despliegue antes siquiera de comenzarlo. LA formación, contratación de nuevo personal y su integración en la estructura debería comenzar tras el caso de negocio y la aprobación del presupuesto. Sería un enorme fracaso que la solución no pudiese ser utilizada adecuadamente o que no es sostenible a largo plazo.

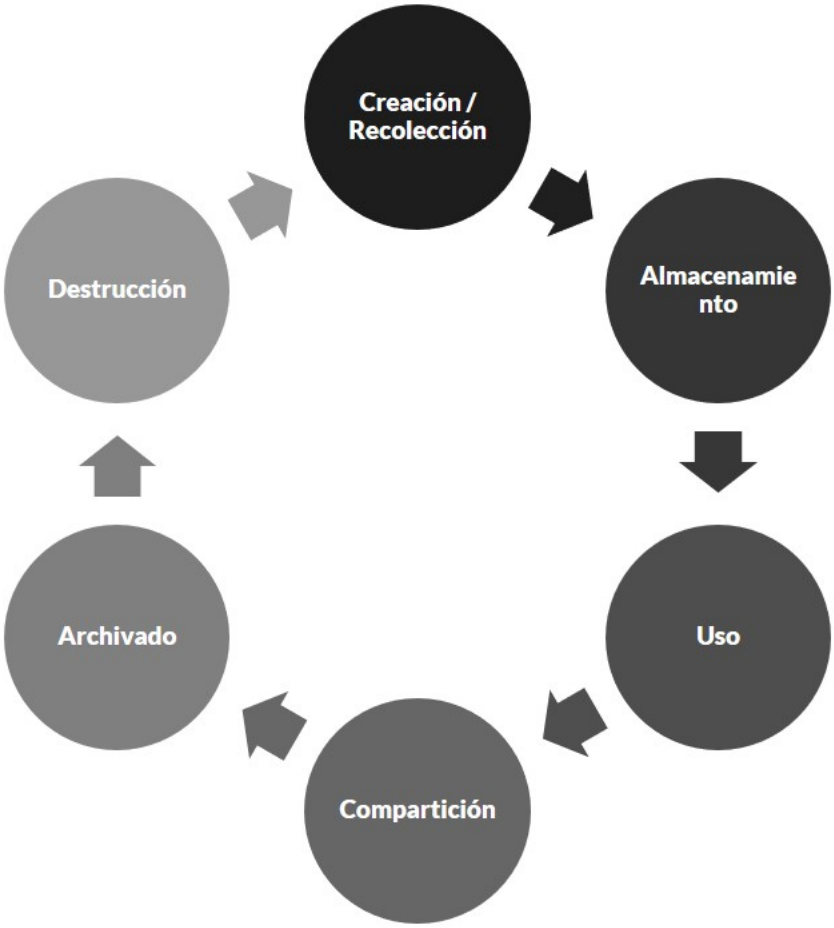
Respecto de los componentes típicos de una arquitectura IAM podemos encontrar los siguientes:

- Repositorio central: Este repositorio centraliza todos los usuarios junto con los roles asignados y las políticas existentes.
- Conectores con las aplicaciones: En el caso de las fuentes autoritativas y secundarias se tratará de una conexión bidireccional (actualizarlas en algunos casos, ser actualizado en otros), y en el de las aplicaciones de negocio undireccional (actualizarlas crendo usuarios con sus permisos de acceso de acuerdo al rol asignado). Estos módulos también permiten pasar a las aplicaciones las credenciales de acceso en caso de SSO.
- Módulo de workflow: Este módulo permite establecer un flujo de trabajo para la aprobación distribuida de las altas, bajas y modificaciones de usuarios y roles.
- Módulo de auto-servicio: Este módulo permite a los usuarios resetear contraseñas (permitiendo varias formas de autenticación como responder a varias preguntas predeterminadas, aplicación en el móvil, etc), y otro tipo de tareas como la petición de nuevos permisos/roles (integrándose así con el módulo de workflow).
- Módulo de autenticación: Encargado de validar a los usuarios con los métodos definidos por tipo de usuario y criticidad de la aplicación (1FA, 2FA etc). Sirve de SSO para evitar múltiples autenticaciones a los usuarios, a la vez que las nuevas aproximaciones permiten realizar una autenticación adaptativa (toma en cuenta diferentes reglas como localización conexión, hora, cumplimiento requisitos seguridad, etc pudiendo hacer más o menos estricta la autenticación en base al perfil de riesgo), generalmente basada en machine learning y analítica para facilitar el proceso (establecer patrones de comportamiento de los usuarios para determinar comportamientos extraños).

- Módulo de autorización: Este módulo establece los permisos de cada usuario de cara a su acceso a las aplicaciones. Existen diferentes aproximaciones, si bien la más común es la basada en roles (RBAC), en la cual se crean diferentes roles basados en las necesidades de negocio de cada usuario (necesidad de saber y menor privilegio), definiendo por cada rol a qué aplicaciones puede acceder y con que tipología de usuario en cada una (limitado por la definición de usuarios de cada aplicación). Es una asignación 1 a n, donde 1 rol en el sistema IAM puede tener múltiples roles en diferentes aplicaciones (permisos de acceso).
- Auditoría y cumplimiento: Este módulo permite realizar un análisis de la información del sistema IAM a la vez que de los accesos realizados con el objeto de general alertas por un lado (p.e acceso a una aplicación no permitida, usuario no ha accedido en un tiempo determinado, etc) así como informes para el cumplimiento interno (políticas y procedimientos) y externo (leyes, regulaciones y cláusulas contractuales).

Protección de la información

La protección de la información es el proceso de salvaguardar la información importante para una organización contra corrupción, compromiso o pérdida. La importancia de esta disciplina es cada vez mayor, toda vez que cada vez se genera más información en las organizaciones, la tolerancia a la indisponibilidad de la misma.
Para la protección de la misma se debe tener en cuenta su ciclo de vida y los posibles estados dentro de la misma en que los datos se pueden encontrar:



El ciclo de vida de los datos sigue los siguientes pasos:

- En la creación y recolección de información es cuando la información es creada o bien se transforma mediante su modificación y/o añadido de nuevos registros.
- En la fase de almacenamiento la información es cuando la información se guarda en reposo en espera de su uso.
- En el uso la información es consumida, aunque no modificada. Ese segundo caso conllevaría la vuelta a la fase de creación o recolección.
- Compartición. La información se hace disponible para otras personas, mediante su envío por email, creación de nuevos usuarios en un sistema, etc.
- Archivado: Almacenamiento a largo plazo de la información con el objeto de dar cumplimiento a obligaciones legales, requisitos internos, etc.
- Eliminación completa de la información cuando ya no es necesaria.

Este ciclo no se basa en pasos secuenciales, sino que cada paso puede llevar a otros, dado que desde su uso se puede pasar a creación y de ahí a almacenamiento y de ahí a compartición, por ejemplo.

Principios de criptografía:

La criptografía es un conjunto de técnicas, que originalmente tratan sobre la protección o el ocultamiento de la información frente a observadores no autorizados. A través de la criptografía la información puede ser protegida contra el acceso no autorizado, su interceptación, su modificación y la inserción de información extra.

- Funciones dentro de la seguridad: Con la criptografía se intenta garantizar las siguientes propiedades deseables en la comunicación de información de forma segura (a estas propiedades se las conoce como funciones o servicios de seguridad):
  - Confidencialidad: solamente los usuarios autorizados tienen acceso a la información.
  - Integridad de la información: garantía ofrecida a los usuarios de que la información original no será alterada, ni intencional ni accidentalmente.
  - Autenticación de usuario: es un proceso que permite al sistema verificar si el usuario que pretende acceder o hacer uso del sistema es quien dice ser.
  - Autenticación de remitente: es el proceso que permite a un usuario certificar que el mensaje recibido fue de hecho enviado por el remitente y no por un suplantador.
  - Autenticación del destinatario: es el proceso que permite garantizar la identidad del usuario destinatario.
  - No repudio en origen: que cuando se reciba un mensaje, el remitente no pueda negar haber enviado dicho mensaje.
  - No repudio en destino: que cuando se envía un mensaje, el destinatario no pueda negar haberlo recibido cuando le llegue.
  - Autenticación de actualidad (no replay): consiste en probar que el mensaje es actual, y que no se trata de un mensaje antiguo reenviado.
- Criptosistemas de clave pública y privada: Existen dos tipos fundamentales de criptosistemas o sistemas de cifrado:

    - Criptosistemas simétricos o de clave privada. Son aquellos que emplean una misma clave k tanto para cifrar como para descifrar. Presentan el inconveniente de que para ser empleados en comunicaciones la clave k debe estar en posesión tanto en el emisor como en el receptor, lo cual nos lleva preguntarnos cómo transmitirles a los participantes en la comunicación esa clave de forma segura.
    - Criptosistemas asimétricos o de clave pública, que emplean una doble clave (kp,kP). kp se la conoce como clave privada y kP se la conoce como clave pública. Una de ellas sirve para la transformación o función E de cifrado y la otra para la transformación D de descifrado. En muchos casos son intercambiables, esto es, si empleamos una para cifrar la otra sirve para descifrar y viceversa. Estos criptosistemas deben cumplir además que el conocimiento de la clave pública kP no permita calcular la clave privada kp. Ofrecen un abanico superior de posibilidades, pudiendo emplearse para establecer comunicaciones seguras por canales inseguros puesto que únicamente viaja por el canal la clave pública, que sólo sirve para cifrar, o para llevar a cabo autenticaciones. Sin la clave privada (que no es deducible a partir de la clave pública) un observador no autorizado del canal de comunicación será incapaz de descifrar el mensaje cifrado.
- Protección de la confidencialidad en información almacenada y en tránsito: En términos generales, hay dos circunstancias en las que se debe usar el usar el cifrado: cuando los datos están “en tránsito” o cuando están “en reposo”. “En tránsito”, en este contexto, es cuando envías información a través de Internet, por correo electrónico, o cuando necesitas almacenarla en otro lugar que no sea tu propio dispositivo. Los datos se consideran “en reposo” cuando se encuentran almacenados en tu dispositivo, ya sea en una parte integrada como un disco rígido, o en un medio extraíble, como una unidad USB. Respecto de este último punto, hay que tener en cuenta varios modelos:
    - Cifrado de disco duro (full disk encryption) o dispositivo: El cifrado de disco duro permite que si el portátil o equipo se pierde por ejemplo, la información contenida en él no pueda ser accedida simplemente montando el disco duro o dispositivo en otra máquina. Tienen la ventaja de ser “transparentes” para el usuario en la medida de que si se ha hecho login correctamente el usuario accede a los documentos de la misma forma que lo haría en un equipo no cifrado. Sin embargo, si se ha hecho login en el equipo o el servidor de ficheros es accesible por el administrador, nada impide a un usuario deshonesto acceder a los datos, copiarlos, reenviarlos, etc. Los datos están protegidos mientras residen en el dispositivo o disco duro, pero dejan de estarlo una vez son extraídos del mismo (copiados a otro dispositivo, reenviarlos, etc.).
    - Cifrado a nivel de fichero: No se cifra una partición o disco duro sino sólo ficheros individuales. Los ficheros cifrados no sólo lo están cuando se encuentran almacenados en el disco, sino que también pueden estar protegidos en tránsito, cuando son enviado por ejemplo como adjuntos en un email. En este caso se pierde el acceso transparente por parte de un usuario y también la protección transparente del mismo. Es decir por ejemplo con PGP, es necesario disponer de la clave púbica de la persona con la que quiero compartir el fichero protegido, y por otro lado, ella deberá tener mi clave pública para poder descifrarlo. Por otro lado, una vez que el documento ha sido descifrado por el receptor, puede almacenarse desprotegido, reenviarse desprotegido, etc.
    - Cifrado de base de datos: Sistemas de base de datos como SQL Server u Oracle utilizan TDE – Transparent Data Encryption para proteger los datos almacenados en bases de datos. Las tecnologías de TDE realizan operaciones de cifrado y descrifrado de datos en tiempo real. Esto permite a los desarrolladores de aplicaciones por ejemplo trabajar con datos sin necesitar modificar las aplicaciones existentes. Este tipo de cifrado protege los datos en reposo en base de datos, pero no cuando estos han sido ya accedidos por la aplicación correspondiente y han podido ser extraídos. Respecto de los administradores, no serán capaces de ver la información si los certificados utilizados para el cifrado son gestionados por otro grupo. Por lo general se cifran columnas concretas con datos sensibles, no toda la tabla (DNI, número de tarjeta, etc).
    - Cifrado a nivel de aplicación. En este caso es la aplicación la que se encarga de cifrar los datos que se almacenarán, en bases de datos, repositorios, etc. Si bien es la técnica más potente y segura, a la vez es la más compleja al tener que añadir funcionalidades de cifrado en el desarrollo de la aplicación, asegurando su implementación correcta. En este caso, sólo los gestores de las claves utilizadas por la aplicación serán capaces de ver todos los datos descifrados. Los usuarios, de acuerdo a sus permisos, serán capaces de acceder a un subconjunto de información.
- Firmas digitales: autenticación, no repudio y protección de la integridad: La firma digital consta de dos “claves” o secuencias de caracteres separadas. Consiste en aplicar mecanismos criptográficos al contenido de un mensaje o documento con el objetivo de demostrar al receptor del mensaje que el emisor del mensaje es real (autenticación), que éste no puede negar que envió el mensaje (no repudio) y que el mensaje no ha sido alterado desde su emisión (integridad). El primer paso es crear un resumen o hash del mensaje. Los funciones de resumen o hash son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija, que representa un resumen de toda la información que se le ha dado (crea una cadena que solo puede volverse a crear con esos mismos datos). Para crear una firma digital, el software de firma crea un hash unidireccional de los datos electrónicos que se deben firmar. La clave privada se usa para encriptar el hash. El hash cifrado junto con otra información es la firma digital. Cualquier cambio en los datos, incluso cambiando o eliminando un solo carácter, da como resultado un valor diferente. Este atributo permite a otros validar la integridad de los datos mediante el uso de la clave pública del firmante para descifrar el hash. Si el hash descifrado coincide con un segundo hash calculado de los mismos datos, prueba que los datos no han cambiado desde que se firmó. Así mismo, al usar la clave privada del emisor, podemos asegurar el no repudio y la autenticación. La única manera de que se pueda descifrar el hash del mensaje con la clave pública de una persona es que se haya usado su clave privada.

Data Loss Prevention e Information Rights Management:

Un aspecto crítico en la protección de datos es la gestión del nivel de acceso de los ficheros no estructurados (aquellos que no se encuentran en una base de datos) y su compartición dentro y fuera de la organización. Para ello se disponen de 2 tipos de soluciones principalmente que pueden complementarse:

- Data Loss Prevention (DLP): Una solución de prevención de pérdida de datos (DLP) es un sistema que está diseñado para detectar potenciales brechas de datos/ transmisiones de datos y prevenirlos a través de monitorización, detección y bloqueo de información sensible mientras está en uso (acciones de extremos), en movimiento (tráfico de red) y en reposo (almacenamiento de datos). La solución no cifra los ficheros, sino que les aplica etiquetas en su descripción de metadatos, y son los agentes desplegados en los equipos/servidores o bien los nodos en red quienes se encargan de bloquear cualquier acción peligrosa. Así, se pueden conceder permisos de grano fico, como leer y editar, pero no copiar/pegar o enviar por mail. En caso de su extracción a disco externo (como USB) se puede bien bloquear, permitir sin problemas (perdiendo el control) o bien aplicándole cifrado para que sólo sea posible verlo en otro equipo controlado por la organización (que disponga del agente). Las políticas generalmente se aplican por roles y/o departamentos y a nivel de repositorios, información con características similares (por ejemplo que contengan la palabra confidencial o números de la seguridad social).
- Information Rights Management: Las tecnologías de IRM (Information Rights Management) permiten el cifrado de documentación aplicando una protección persistente a los mismos. La documentación en reposo se encuentra cifrada y sólo está accesible a los usuarios que tengan derechos de acceso a la misma. Los derechos por lo general se dan de forma granular y se asignan usuario a usuario, por lo que es más recomendable de cara a la compartición de ficheros con terceras partes. Así, se puede compartir un fichero con sólo permisos de lectura, o también de modificación, pero por ejemplo no de compartición, copia o impresión. Así mismo, los permisos pueden ser cambiados o eliminados en tiempo casi real. Para el acceso a la información por sus receptores, se requiere de un cliente que accederá al servidor de permisos cada vez que se abra el fichero para comprobar qué se puede hacer (algunas soluciones permiten su acceso online sin modificación y sólo para cierto tipo de ficheros como PDF u office).

Seguridad en el correo electrónico:

El correo electrónico es uno de los principales medios de compartición de información, tanto a nivel interno de la organización como externa, a la vez que uno de los principales vectores de entrada para amenazas (correos phishing). Por ello, se deben contar con sistemas que permitan obtener las siguientes funcionalidades:

- Detección de phishing: Mediante técnicas como detección de orígenes, inteligencia artificial aplicada al análisis del contenido, etc, detectar que se tarta de un posible caso de phishing.
- Detonación de ficheros y enlaces: Capacidad de poder analizar enlaces y adjuntos en correos electrónicos mediante el uso de sandboxes para validar su comportamiento.
- Análisis de malware: Capaz de poder utilizar técnicas de firmas y de inteligencia artificial para validar si un fichero adjunto es un malware.
- Control de información saliente (DLP): Análisis del contenido de los correos y los adjuntos para, sólo o en conjunción con una solución DLP. Poder evitar fugas de información. Otra opción sería el cifrado del correo y/o los adjuntos, de forma que solo el destinatario legítimo podría verlo.
- Detección de fraudes y buzones comprometidos: Capacidad de detectar actividad anómala en buzones y posibles casos de fraude como el fraude del CEO.

- Detección de exploits: Análisis de comportamiento al abrir enlaces y/o adjuntos para detectar posibles explotaciones del sistema para desplegar malware, tomar el control del sistema, etc.

Monitorización de actividad en BBDD y almacenes de datos:

Las bases de datos y los repositorios de ficheros son objetivos primordiales para los atacantes debido a la sensibilidad de la información contenida de manera general. Por ello, un método de proteger los datos es monitorizar la actividad realizada en los mismos a bajo nivel con el objeto de descubrir posibles comportamientos sospechosos o directamente delictivos. Una solución de este tipo debería ofrecer la siguiente funcionalidad:

- Automatizar el descubrimiento y la clasificación de datos sensibles: Es vital que una solución de este tipo permita analizar el tráfico y los repositorios/bases de datos a las que tiene acceso con el objeto de encontrar tanto nuevos repositorios como nueva información susceptible de protección.
- Monitorización en tiempo real actividad de los usuarios: Debe ser capaz de poder analizar la actividad a nivel granular y auditarla para diferentes repositorios, bases de datos SQL y no SQL, data warehouses, etc.
- Soporte al cumplimiento legal y normativo (plantillas predefinidas): Debe incluir plantillas para auditar y reportar el cumplimiento legal y normativo para diferentes de estas como RGPD, PCI-DSS, HIPAA, SOX, etc.
- Políticas predefinidas y adaptables: Debe incluir por defecto multitud de políticas adaptables para auditar y bloquear actividades sospechosas y/o potencialmente peligrosas.
- Bloqueo de acciones y enmascaramiento de datos: Debe permitir actuar como un cortafuegos de capa 7 (de aplicación) con el objeto de bloquear acciones que se hayan definido previamente, a la vez que permite otras acciones enmascarando los datos (cubriendo una parte de los mismos por protección, por ejemplo para la protección de datos personales.

Seguridad operacional

Las operaciones de los sistemas, su administración y explotación requieren de controles de seguridad específicos para asegurar que dicha operación no introduzca nuevas debilidades y permita controlar las existentes.

Configuración segura o hardening:

El hardening o configuración segura es el proceso de configuración sistemática de los sistemas y aplicaciones (firmware, SO, BBDD, aplicaciones de negocio, etc) con el objeto de reducir la superficie de ataque potencial así como seleccionar opciones que aumenten la seguridad general del sistema y la información.

Existen multitud de guías de fabricantes para realizar dicha tarea, así como guías de organizaciones internacionales como el Center for Internet Security.

En general, este proceso se centra en aspectos como cerrar puertos innecesarios en los sistemas, asegurar las políticas de acceso de usuarios (como contraseñas seguras o los factores de autenticación necesarios), la habilitación de cifrado, configuración de las capacidades de seguridad nativas de cada sistema/aplicación, permisos de seguridad en archivos y carpetas, acceso remoto, etc.

Para permitir automatizar este proceso, existen soluciones que permiten validar la configuración de un sistema contra una línea base establecida (análisis de cumplimiento) y otro tipo que permite cambiar las configuraciones de sistemas y aplicaciones para cumplir con la línea base (enforcement).

Gestión de vulnerabilidades:

Una vulnerabilidad (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. La gestión de vulnerabilidades es un proceso continuo de TI consistente en la identificación, evaluación y corrección de vulnerabilidades en los sistemas de información y las aplicaciones de una organización, categorizando los activos según si importancia/valor y clasificando las vulnerabilidades según el nivel de riesgo, de forma que se puedan priorizar las vulnerabilidades a corregir (por lo general existen más vulnerabilidades que capacidad de mitigarlas/corregirlas).
El proceso de gestión de vulnerabilidades suele incluir las siguientes acciones:

- Obtención de un inventario (y categorización por nivel de criticidad) de los activos de TI de una empresa, lo que incluye servidores, infraestructura de redes, estaciones de trabajo, impresoras y aplicaciones.
- Detección de las vulnerabilidades existentes mediante escáneres de redes, escáneres de vulnerabilidades en host y software de pruebas de penetración automáticas (o pruebas manuales) y determinación de los niveles de riesgo. Generalmente, los escaneos en red suelen dar más falsos positivos que los realizados con agentes (puesto que no pueden probar determinados aspectos o bien no tienen acceso al sistema para validar condiciones necesarias para explotar una vulnerabilidad).
- Reparación de sistemas y dispositivos vulnerables y presentación de informes sobre las medidas correctivas adoptadas. Este sub-proceso debe alinearse con la gestión del cambio para evitar impactar en los sistemas y contar con procedimientos específicos como contar con un plan de vuelta atrás antes de aplicar cambios en prueba en entornos de pre-producción antes de su despliegue definitivo.

Gestión del cambio

Los procesos de cambio pueden conllevar riesgos asociados para la seguridad de la información. Es por ello que se deben disponer de procesos y controles para que analicemos los procesos de cambio en sistemas y aplicaciones, junto con la infraestructura involucrada con los mismos.

Las evaluaciones de riesgos deberían exigir siempre una autorización formal para la realización de cambios. Otro elemento esencial es establecer siempre una planificación para los cambios a realizar en equipos, sistemas software etc, acompañado de pruebas realizadas y comunicaciones a todos los involucrados.

Antes de realizar ningún cambio se debe disponer de un procedimiento de vuelta atrás (definición de cómo volver al estado anterior en el sistema/aplicación en caso de problemas con el cambio realizado) así como de probar los cambios en un entorno de pruebas lo más parecido al entorno de producción (para evitar discrepancias que podrían provocar impactos en el entorno de producción no detectados en el de pruebas).

Finalmente, deberíamos mantener un registro que contenga al menos la información de:

- Quien autoriza los cambios.
- Quien realiza los cambios.
- Fecha.
- Descripción de las tareas realizadas.
- Validación del cambio.
- Otra información que se considere necesaria.

Esta información será útil en una auditoría para proporcionar la confianza de que los cambios se han realizado de forma controlada.

Gestión de la capacidad

Se trata de evitar pérdidas de disponibilidad o rendimiento de los sistemas por falta de capacidad. Gestionar la capacidad se refiere a tener un control del uso de los recursos.

Esto se traduce en controles para:

- Medición y Seguimiento del uso de recursos.
- Previsión de uso a futuro (prever “cuellos de botella”) o análisis de tendencias.
- Planificar las ampliaciones de capacidad de los recursos cuando sea necesario.
- Optimizar el uso de recursos. Por ejemplo, la posibilidad de optimizar las consultas a las bases de datos, realizar procesos por lotes fuera de horas de carga de trabajo, eliminación de archivos de datos antiguos y aceleración del ancho de banda para accesos no críticos.

Para poder monitorizar la capacidad existen sistemas de monitorización de salud TI que permiten automatizar estas tareas en SO, BBDD, dispositivos de red, aplicaciones comerciales (así como en desarrollos o personalizaciones propias mediante la creación de agentes que se integren con el sistema de monitorización), etc.

En estos sistemas se deben definir, por cada elementos monitorizado, umbrales de alerta y de alarma (los primeros indicarían que se está llegando a una situación límite y el segundo que dicha situación ha ocurrido).

Control del software en explotación

El objetivo es garantizar la integridad de los sistemas operacionales para la organización. Es importante mantener procedimientos para cubrir las instalaciones de software en cualquier dispositivo dentro de una organización.

Estos procedimientos deben fijarse en la aplicabilidad de los siguientes controles

- Probar las nuevas aplicaciones o software en entornos aislados especialmente preparados para pruebas.
- Comprobar las necesidades de instalación (compatibilidad del entorno) antes de su instalación.
- Valorar la necesidad de actualización o instalación.
- Planificar la forma de volver a versiones anteriores en caso de ser necesario.
- Los entornos de desarrollo deben permanecer aislados de los entornos operativos.
- Las instalaciones de software debe ser realizada por usuarios autorizados.
- Establecer procedimientos o herramientas de monitoreo del software para detectar cambios no autorizados.
- Las pruebas posteriores a la implementación deben incluir una supervisión de la red para identificar cualquier tráfico inesperado que pueda exponer errores o suponga empeoramiento de la velocidad de las transmisiones.

Protección contra malware y del punto final:

La protección del punto final se basa en proteger la infraestructura final (como sistemas y servidores) así como las aplicaciones desplegadas en los mismos con el objeto de evitar un punto de entrada a la información almacenada (o bien que sirvan como un punto de salto a otros sistemas con información más interesante para el atacante, se puedan robar credenciales que se reutilicen, se pueda utilizar el correo del afectado para un fraude, etc).

Protección antimalware:

Los antivirus son programas cuyo objetivo es detectar y eliminar virus informáticos. Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e internet, los antivirus han evolucionado hacia programas más avanzados que además de buscar y detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de los mismos.

Actualmente son capaces de reconocer otros tipos de malware como spyware, gusanos, troyanos, rootkits, RATs, etc. Históricamente se basaban en firmas, de manera que se necesitaba en los fabricantes hubiesen creado (o recibido de otros, dado que compartían), dicha firma. Esto ya no es válido, dado que es fácil modificar un virus para que su firma no genere una alarma, además de que muchas veces cuando se tiene una firma ya es tarde (p.e wannacry).

Los nuevos sistemas se basan en aprendizaje máquina o aprendizaje profundo de forma que se entrena a los sistemas para que detecten características que comparten los malware, de forma que son capaces de dectarlos sin firmas, aunque sean nuevos (si bien ya comienzan a encontrarse ficheros con modificaciones suficientes para engañar a estos sistemas).

Otros sistemas se basan en detectar las características de una explotación, de forma que prevengan que el malware pueda tomar control del sistema, cifrar el disco duro, elevar privilegios, etc.

Endpoint Detection & Response:

Este tipo de soluciones se encargan de monitorizar los sistemas donde están desplegados los agentes, analizando los procesos que se crean, trazas de memoria, conexiones de red entrantes y salientes, etc, para detectar posibles ataques hacia o desde el sistema. Aborda la necesidad de una supervisión en tiempo real, centrarse en los análisis de seguridad y en la respuesta al incidente.

Ofrece una visibilidad completa de extremo a extremo sobre la actividad de cada equipo, administrada desde una única consola, junto con una valiosa inteligencia de seguridad que podría usar un experto de seguridad informático para una investigación y respuesta mayores.

El objetivo principal de EDR es la detección proactiva de amenazas nuevas o desconocidas, infecciones previamente no identificadas que penetran en la organización directamente a través de endpoints y servidores. Ofrecen las siguientes capacidades:

- Modelo preventivo (pre-infección) y detectivo (post-infección) basado en análisis sobre patrones de comportamiento.
- Enfoque reactivo (post-incidente) apoyado en capacidades de contención y remediación rápida frente incidentes (segundo o minutos).
- Capacidades forenses, basadas en análisis sobre el registro de actividades del endpoint (tráfico de red, procesos, etc.).
- Inteligencia agregada, a través de un proceso continuo de investigación e innovación gracias a nuestro laboratorio y analistas expertos

Otras soluciones de seguridad en punto final:

- FIM: La monitorización de integridad de fichero o FIM emplea uno o varios algoritmos de hash se extraen los «message digest» o resúmenes de un archivo o archivos críticos del sistema y se almacenan en una base de datos o archivo maestro («línea base»). De forma regular, se ejecutan extracciones de «resúmenes y se comparan contra la «línea base» con el fin de detectar posibles modificaciones, generando alertas a los administradores si esto ocurre. Esta es una forma fácil y confiable de garantizar la integridad de la configuración y los datos en sistemas informáticos y complementar los controles asociados a la gestión de cambios («Change Management») y trazabilidad. Esto por ejemplo es importante en los ficheros de configuración, ficheros críticos de DLL, etc para poder detectar modificaciones indebidas que denotarían una posible brecha (como instalación de una puerta trasera).
    - Protección de móviles: Los smartphones, ya sean corporativos, o personales a los que se se les permite acceso a la información corporativa, deben ser protegidos. Esta tipo de soluciones deben contar con protección antivirus (no para iPhone), cifrado de datos, correo electrónico seguro, creación de espacios

de trabajo separados (el personal, y el de trabajo con el calendario, datos y correo cifrado), gestión remota (actualizaciones, cambio de políticas, borrado/bloqueo en caso de robo), etc.
    - Tecnología de señuelos: Este tipo de tecnología es capaz de crear sistemas señuelo en la red incluyendo información falsa adaptada al tipo de información gestionada por la organización. Esto sirve tanto para detectar de manera inequívoca que se está produciendo un ataque (al no ser un sistema de negocio, nadie debe entrar al mismo) como para poder analizar el ataque realizado y aprender del adversario. Hoy en día existe tecnología que despliega sistemas tontos, y en caso de ataque permite levantar un sistema completo para engañar al atacante (anteriormente los sistemas tontos eran fáciles de detectar, pero disponer de una infraestructura de sistemas completo era inviable por el costo de licencias. Aquí se tiene lo mejor de ambos mundos).
    - Seguridad en la virtualización: La tecnología de virtualización, tanto la clásica (como VMWare) como la basada en contenedores (como Kubernetes), supone un nuevo paradigma, de forma que se debe proteger no solo la máquina física, sino las máquinas virtuales/contenedores que dependen de ella. Por ello, la tecnología de seguridad debe adaptarse a este nuevo entorno, teniendo en cuenta aspectos como la monitorización de tráfico en redes virtuales (en algunos casos, el tráfico entre máquina virtuales nunca pasa por interfaces de red físicas, por lo que diferentes soluciones tradicionales estarán ciegas).

Copias de seguridad:

Una copia de seguridad es un proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperarlos en caso de fallo del primer alojamiento de los datos (tanto a nivel completo en caso de desastre, como parcial en caso de corrupción o perdida de unos ficheros).

- Para determinar la frecuencia con la que debemos realizar copias de seguridad, será necesario realizar un análisis en el que se tengan en cuenta los siguientes factores:
    - Número de datos o archivos generados y/o modificados en la organización.
    - Impacto para el negocio de la perdida de datos por unidad de tiempo (una hora, un día, una semana, un mes, etc).
    - Coste de almacenamiento.
    - Obligaciones legales y normativas.
- Otro temas a tener en cuenta es el periodo de retención de los datos, cuánto tiempo debemos mantener las copias de seguridad, a decidir en base a requisitos legales y necesidades de la organización.
- También es crítico decidir el tipo de copia de seguridad a realizar:
    - Copia de seguridad completa: Cuando se realiza una copia de seguridad completa todos los archivos y carpetas del sistema se copian. Por lo tanto tu sistema de copias de seguridad almacena una copia completa que es igual a la fuente de datos del día y hora en que se hace la copia de seguridad. Aunque el tiempo que se necesita para hacer esta copia de seguridad es mayor y requiere más espacio de almacenamiento, tiene la ventaja de que con una copia de seguridad completa la restauración es más rápida y más simple.
    - Copia de seguridad incremental: En este caso, la única copia completa es la primera. A partir de ahí, las copias de seguridad posteriores sólo almacenan los cambios realizados desde la copia de seguridad anterior. En este caso el proceso de restauración es más largo porque tienes que utilizar varias copias diferentes para restaurar completamente el sistema, pero a cambio el proceso de hacer la copia de seguridad es mucho más rápido y ocupa menos espacio de almacenamiento.
    - Copia de seguridad diferencial: Igual que las incrementales, la primera copia de seguridad es la única completa. La diferencia con la incremental viene del hecho de que aquí cada copia de seguridad posterior tiene todos los cambios respecto a la primera copia completa, y no respecto a la copia de seguridad anterior, como era el caso de la incremental. Por lo tanto en este caso la copia de seguridad requiere más espacio de almacenamiento que las incrementales, pero con la ventaja de que el tiempo de restauración es menor.
    - Copia espejo (mirroring): Con una copia de seguridad en espejo se realiza una copia exacta de los datos originales. Se suele hacer “en directo”, es decir, a la vez que trabajas con los datos reales, se hace una copia espejo en un disco alternativo. La ventaja de una copia en espejo es que la copia de seguridad no contiene archivos antiguos o en desuso. Pero esto también puede ser un problema ya que si un archivo se elimina accidentalmente en el sistema original, el sistema espejo lo elimina también. Generalmente se utiliza en sistemas con requisitos de disponibilidad elevados y que cuentan con sitios espejos (sistemas en activo que pueden tomar el lugar de los sistemas originales en cuestión de segundos).
- Se deben contar con procedimientos de recuperación y probar de forma regular tanto los procedimientos como las copias con el fin de asegurar que en caso de necesidad no existirá problema, como que las copias de seguridad no se habían realizado correctamente y no es posible recuperarlas o que en el procedimiento se han olvidado incluir pasos críticos.
- Por último, pero no menos importante, hay que tener muy presente que se deberán proteger las copias de seguridad con el mismo nivel de controles que la información original (con el objeto de evitar que se conviertan en un agujero), y tener en cuenta que es necesario disponer de copias en sitios geográficamente alejados del sitio donde se alojan los datos originales en caso de desastre (otra ubicación de la organización, un tercero contratado específicamente o la nube).

Monitorización de eventos y supervisión

El objetivo es registrar los eventos relacionados con la seguridad de la información y generar evidencias. Para ello es necesario realizar las siguientes actividades:

- Registro y gestión de eventos de actividad: Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.
- Protección de los registros de información: Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.
- Registros de actividad del administrador y operador del sistema: Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular.
- Sincronización de relojes: Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o de un dominio de seguridad y en relación a una fuente de sincronización única de referencia.

Deberemos mantener un registro de los eventos, para en caoi de incidente poder determinar qué estaba sucediendo mediante los datos de la hora, la fecha del incidente, etc., las personas involucradas, el origen y las causas, etc. Entre los eventos a monitorizar podemos encontrar:

- Intentos de acceso exitosos y fallidos,
- Desconexiones del sistema
- Acciones ejecutadas,
- Alertas por fallos en el sistema
- Fecha y hora en que se producen los eventos
- Tiempos de detención
- Etc.

Este tipo de control es complicado de realizar en empresas medianas y grandes en caso de no disponer de un sistema centralizado para realizar estas tareas, como sería un SIEM.

Se trata de un tipo de herramienta de seguridad que permite recolectar eventos de seguridad desde diferentes fuentes (SO, FWs, IDS, AV, etc) en un formato unificado con el objeto de poder correlacionarlos y analizar posibles intrusiones o problemas de seguridad que afecten a diferentes tipos de sistema y de forma centralizada. Su principal funcionalidad es la siguiente:

- Disponer de reglas de alerta y correlación para notificar posibles intrusiones y el cumplimiento normativo.
- Disponer de un sistema de análisis avanzado de los eventos para los gestores de incidentes.

- Capacidad de análisis de comportamiento de usuarios y entidades (UEBA) que permite establecer patrones estadísticos avanzados del comportamiento de usuarios y dispositivos con el objeto de alertar de anomalías que podrían ser indicadores de un ataque.
- Capacidad de análisis de comportamiento y análisis forense en red (NBA) para establecer patrones estadísticos avanzados del tráfico general de la red y poder detectar anomalías.
- Permitir la integración u ofrecer un sistema de orquestación, automatización y respuesta de seguridad (SOAR) para definir pasos de respuesta ante tipologías de incidentes así como la automatización de determinados pasos (detonación de ficheros, recopilación de información, bloqueo en un cortafuegos, aislamiento en la red de un sistema o conjunto de sistemas, etc).

Consideraciones para la auditoría de SI

Estos controles buscan minimizar el impacto de las actividades de auditoría en los sistemas operativos mediante la planificación de actividades de forma que causen la mínima interferencia en los sistemas operativos.

No estamos hablando de auditorías generales (como las de cumplimiento normativo) sino de auditorias de los sistemas de información para evaluar cosas como:

- ¿Los usuarios están trabajando con los privilegios correctos?
- ¿La infraestructura es estable y confiable?
- ¿Las infraestructuras cuentan con la suficiente capacidad (memoria, procesamiento, almacenamiento, ancho de banda)?
- ¿Cómo puede ser mejorado?
- ¿Las pruebas realizadas son efectivas?
- ¿Cuán efectivas son las actividades de mantenimiento, monitoreo y gestión?
- ¿Qué hacen los usuarios del sistema?

En este aspecto deberemos controlar que las auditorias para obtener esta información:

1. Cumplan con el alcance planificado. En la práctica el alcance de las auditorias puede ser demasiado abierto de forma que la auditoría podría convertirse en una enorme tarea que reduce su propio valor, perdiendo un enorme esfuerzo en cosas que son de poca importancia. Delimitar las auditorias es una primera y primordial tarea para no devaluar su significado y para que realmente sean útiles.
2. Evaluar y considerar el impacto. Se debe evaluar el impacto o consumo de recursos de auditorías que supongan un consumo de recursos importante dentro de los sistemas. En este caso debe existir un procedimiento por el cual se evite realizar estas tareas que pueden comprometer la capacidad de los sistemas realizándolas en periodos de baja carga de trabajo.

Seguridad de las comunicaciones

Los sistemas, aplicaciones e información de las organizaciones se encuentran desplegadas en redes informáticas que facilitan su comunicación, tanto a nivel interno como externo. Así, en la red se pueden originar nuevas amenazas que deben ser paradas, a la vez que aporta información que puede ayudar a detectar un ataque en curso.

Segmentación y microsegmentación de la red:

La segmentación de la red consiste en dividir una gran red (como puede ser la intranet, una extranet, etc) en segmentos más pequeños, filtrando por cada uno de ellos las entradas y salidas de tráfico de red, de forma que se facilite minimizar la superficie de exposición de los sistemas en el interior. Ls criterios para la selección de sistemas a incluir en un segmento puede tomar en cuenta aplicaciones con un nivel de criticidad mayor que su entorno, sistemas con funcionalidades complementarias, entornos de un sistema, etc. Esta segmentación se suele realizar de manera física o bien lógica (siendo el mecanismo más utilizado en uso de VLANs o redes virtuales), si bien tiene una limitación sobre el número de subredes que se pueden tener (al gestionarse mediante electrónica de red que se acaba saturando.

Para poder llegar a un nivel superior de segmentación, se creo el término micro-segmentación, donde el objetivo es llegar a segmentar por servicios dentro de una misma aplicación, de forma que casi cada sistema cuenta con su propio segmento y reglas de filtrado. Para poder llegar a tal nivel, se introdujo un nuevo tipo de tecnología, Red Definida por Software (SDN), un conjunto de técnicas relacionadas con el área de redes computacionales, cuyo objetivo es facilitar la implementación e implantación de servicios de red de una manera determinista, dinámica y escalable, evitando al administrador de red gestionar dichos servicios a bajo nivel (mediante la separación del plano de control, software del plano de datos, hardware).

Por lo general este tipo de productos cuentan con sistemas de análisis que permiten poner la red en modo escucha para que ofrezcan un posible mapa de segmentos y reglas de filtrado que a continuación podrá ser refinado por la organización (en lugar de comenzar desde cero que sería un trabajo enorme dado el número de sistemas en empresas grandes y multinacionales).

IDS/IPS (Detección/Prevención de intrusiones en red):

Un sistema de detección de intrusiones (IDS) es un programa de detección de accesos no autorizados a una red. Se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El IDS no solo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento. Un IPS (prevención) añade capacidad de bloqueo del tráfico de acuerdo a reglas predefinidas.

En el caso de tráfico cifrado, para analizarlo (como en otras soluciones como cortafuegos), se puede utilizar técnicas de man in the middle (el dispositivo se coloca en la mitad suplantando al otro miembro en cada conversación, de forma que ambos utilicen sus certificados) o bien cargar los certificados de cifrado de todos los sistemas a analizar su tráfico.

Dado que los sistemas de firmas tienen los mismos problemas que los antivirus, un nuevo modelo basado en aprendizaje máquina y aprendizaje profundo ha surgido para poder detectar ataques en la red mediante análisis de anomalías y características similares de ataques.

Cortafuegos (FWs):

Un cortafuegos (FW) es la parte de una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas, todo mediante reglas definidas. En base a este principio, se recomienda definir qué está permitido y bloquear el resto (whitelisting) que definir lo que no está permitido y permitir el resto (blacklisting).

Los FW han evolucionado en los siguientes modelos:

- A nivel de paquetes: En este caso se crean reglas para paquetes de datos, debiendo crear reglas en ambos sentidos, lo cual era un problema de seguridad (se puede permitir el acceso en la dirección contraria del flujo de datos).
- Con estado: En este caso se mantenía una tabla dentro del FW que controlaba las sesiones creadas, de forma que sólo era necesario crear una regla del origen al destino, permitiendo el paso al resto de paquetes que fuesen parte de la sesión.
- A nivel de aplicación: Son aquellos que actúan sobre la capa de aplicación pudiendo entender entender ciertas aplicaciones y protocolos (por ejemplo FTP, DNS o HTTP), y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial. El

ejemplo más claro es el WAF que permite proteger aplicaciones web frente a ataques como SQL Injection o XSS.
- Con inspección profunda de paquetes (DPI): El DPI combina las funciones de un sistema de detección/prevención de Intrusiones (IDS/IPS) con un tradicional cortafuegos de estado permitiendo detectar ciertos ataques que ni los sistemas de detección de intrusiones ni los sistemas de prevención de intrusiones ni los cortafuegos de estado pueden detectar por sí solos. Así por ejemplo, es capaz de asociar sesiones a usuarios y a protocolos (sin importar el puerto utilizado) y filtrar por estos aspectos.
- Software Defined Firewall: Con el advenimiento de las redes definidas por software, un nuevo tipo de cortafuegos nació definido a través de las reglas de control del SDN, de forma que se libera el cortafuegos del plano de datos.

Seguridad en la adquisición, desarrollo y mantenimiento de SI

El objetivo es:

- Asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.
- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura base en la cual se apoyan.
- Definir los métodos de protección de la información crítica o sensible.

El diseño e implantación de los sistemas de información que sustentan los procesos de negocio son cruciales para la seguridad. Esto aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software que integren cualquiera de los entornos administrados por la organización en donde residan los desarrollos mencionados (BBDD, servidores web/aplicaciones, librerías, etc). Es importante que todos los entornos donde los sistemas estén desplegados cumplan los mismos requisitos que el de producción (como desarrollo, pruebas/calidad, etc), a no ser que se pueda asegurar que los entornos no productivos no dispondrán de información productiva (está anonimizada o mezclada de forma que no tiene valor para un atacante), que los entornos están perfectamente segmentados (separados entre ellos, por ejemplo mediante VLANs) y que no existe comunicación directa entre los mismos.

Los requisitos de seguridad deben ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información. Todos los requisitos de seguridad deben identificarse en la fase de recogida de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información.

El modelo de protección en capas debe ser el seleccionado, asegurando que existen diferentes controles que permitan aportar diferentes barreras en caso de que uno se ellos sea sobrepasado.

Se debe garantizar la seguridad de la información en los entornos de diseño e implementación dentro del ciclo de vida de desarrollo de los sistemas de información:

- Política de desarrollo seguro de software: Se deberían establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización.
- Procedimientos de control de cambios en los sistemas: En el ciclo de vida de desarrollo se deberían hacer uso de procedimientos formales de control de cambios.
- Revisión técnica de las aplicaciones tras efectuar cambios en el sistema: Las aplicaciones críticas para el negocio se deberían revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización tras la realización de cambios.
- Restricciones a los cambios en los paquetes de software: Se deberían evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente.
- Uso de principios de ingeniería en protección de sistemas: Se deberían establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.
- Seguridad en entornos de desarrollo: Las organizaciones deberían establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.
- Externalización del desarrollo de software: La organización debería supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado, estableciendo a la vez cláusula de seguridad en los contratos (p.e controles de seguridad en los entornos, inclusión de requisitos y diseño de seguridad, pruebas a realizar, posibilidad de auditar al tercero, etc).
- Pruebas de funcionalidad durante el desarrollo de los sistemas: Se deberían realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.
- Pruebas de aceptación: Se deberían establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.

Por último, los datos de pruebas se deberían seleccionar cuidadosamente y se deberían proteger y controlar.

Para poder automatizar parte del proceso, existen herramientas que pueden facilitar dicho trabajo.

Primero destacar las herramientas de análisis de vulnerabilidades y test de intrusión. estas pueden ser integradas de forma manual, o automatizarse su ejecución en un modelo de CI/CD (devops):

- Análisis de vulnerabilidades de SO y aplicaciones comerciales (BBDD, librerias, servidores web, etc).
- Análisis de vulnerabilidades en aplicaciones web.
- Test de intrusión automatizados en aplicaciones.
- Auditoría de código fuente.

Las aplicaciones Runtime Application Self-Protection (RASP) o aplicaciones de autoprotección en tiempo de ejecución se integran dentro de las aplicaciones web, siendo capaz de conocer sus puntos vulnerables y de proteger las peticiones de entrada con datos de entrada maliciosos que se dirijan a estos puntos. Trabaja de manera autónoma y es capaz de inferir la lógica de negocio de la propia aplicación y conocer lo que debe proteger. Esto evita los problemas de administración y gestión de reglas que ocurren en los cortafuegos a nivel de aplicación. Esto sería un complemento (o trabajar sólo) a los cortafuegos a nivel de aplicación visto en la sección de seguridad en comunicaciones.

Existen también aplicaciones que permiten la gestión segura de librerías de terceros y open source con el objeto de detectar librerías deprecadas o con vulnerabilidades conocidas. Dado que un desarrollo dese cero es casi imposible, el uso de librerías es cada vez más común. Si bien este enfoque permite una mayor agilidad y eficiencia, debemos asegurar que no se convierte en un vector de vulnerabilidad para los sistemas.

Continuidad de negocio y recuperación ante desastres

El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad. Se deberían integrar dentro de los procesos críticos de negocio aquellos requisitos de gestión de la seguridad de la información con atención especial a la legislación, las operaciones, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativos y/o que estén dispuestos de un modo distinto a la operativa habitual.

Se debe distinguir entre continuidad de negocio, que permite la continuación del negocio en general en caso de desastre, y el plan de recuperación, que facilita la vuelta atrás en caso de desastre (reconstrucción de los sistemas en el orden de prioridad necesario).

Entre los controles necesarios podemos hallar los siguientes:

- Continuidad de la seguridad de la información: El objetivo es que la seguridad de la información sea integrada en los sistemas de gestión de la continuidad del negocio de la organización.
  - Planificación de la continuidad de la seguridad de la información: La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.
  - Implantación de la continuidad de la seguridad de la información: La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.
  - Verificación, revisión y evaluación de la continuidad de la seguridad de la información: La organización debería verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.
- Redundancias: El objetivo es asegurar la disponibilidad de los recursos de tratamiento de la información. Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.

Entre las diferentes estrategias para la recuperación ante desastres, podemos encontrar las siguientes:

- Espera pasiva (cold sites). Se basa en centros donde se pueden contratar servidores en caso necesario, pero se deben desplegar los mismos así como los sistemas y configurar todo. La organización envía regularmente copias de seguridad para una reconstrucción completa a almacenamientos externos (a una distancia prudencial para evitar que desastres amplios como un terremoto pudiese afectar a la capacidad en centros cercanos al principal). Esta estrategia puede llevar días o semanas y sólo es recomendable para aplicaciones con bajos requisitos de disponibilidad (RTO).
- Espera semiactiva (warm sites). En este caso se dispondría de servidores desplegados con las aplicaciones base también desplegados y sería necesario realizar la carga de los datos y finalizar las últimas configuraciones. Esta estrategia llevaría desde unas horas a unos pocos días (dependiendo de la complejidad del entorno) y puede servidor para aplicaciones que no sean especialmente críticas (se recuperaría primero las más criticas y en orden el resto).
- Espera activa (hot sites): Se trata de centros espejo donde todas las configuraciones y datos de las aplicaciones se encuentran replicadas en tiempo real. Esta estrategia es muy cara pero efectiva para aplicaciones muy críticas, dado que permite tiempos de indisponibilidad nulos o de minutos (dependiendo de si se encuentran en activo-activo o activo-pasivo).

Hoy en día, gracias a la nube, es mucho más sencillo disponer de una estrategia de recuperación ante desastres, ya sea con los sistemas principales en la nube (estrategia sencilla y que el propio proveedor puede soportar) o bien con los sistemas en local y el respaldo en la nube (más problemático, pero permite un mayor control de los sistemas si existen requisitos para tenerlos on premise de forma general).

Los elementos esenciales para un plan sólido de recuperación ante desastres son estos:

- Definición del plan: Para que un plan de recuperación ante desastres funcione, tiene que involucrar a la gerencia. Ellos son los responsables de su coordinación y deben asegurar su efectividad. Adicionalmente, deben proveer los recursos necesarios para un desarrollo efectivo del plan. Todos los departamentos de la organización participan en la definición del plan.
- Establecimiento de prioridades: A continuación, la organización debe preparar un análisis de riesgo y crear una lista de posibles desastres naturales o causados por errores humanos, y clasificarlos según sus probabilidades. Una vez terminada la lista, cada departamento debe analizar las posibles consecuencias y el impacto relacionado con cada tipo de desastre. Esto servirá como referencia para identificar lo que se necesita incluir en el plan. Un plan completo debe considerar una pérdida total del centro de datos y eventos de larga duración de más de una semana.
  Una vez definidas las necesidades de cada departamento, se les asigna una prioridad. Esto es importante, porque ninguna compañía tiene recursos infinitos. Los procesos y operaciones son analizados para determinar la máxima cantidad de tiempo que la organización puede sobrevivir sin ellos. Se establece un orden de recuperación según el grado de importancia. Esto se define como el Recovery Time Objective, Tiempo de Recuperación o RTO. Otro término importante es el Recovery Point Objective, Punto de Recuperación o RPO (mediante el desarrollo del BIA visto anteriormente).
- Selección de estrategias de recuperación: En esta etapa se determina las alternativas más prácticas para proceder en caso de un desastre. Todos los aspectos de la organización son analizados, incluyendo hardware, software, comunicaciones, archivos, bases de datos, instalaciones, etc. Las alternativas a considerar varían según la función del equipo y pueden incluir duplicación de centros de datos, alquiler de equipos e instalaciones, contratos de almacenamiento y muchas más. Igualmente, se analiza los costos asociados. La virtualización representa un avance considerable al aplicarse en el Plan de Recuperación ante Desastres (DRP). Según una encuesta de Acronis, las razones principales por las que se adopta la virtualización en un DRP son: eficiencia mejorada (24%); flexibilidad y velocidad de implementación (20%) y reducción de costos (18%). Esta virtualización iría mano con mano con la nube (si bien se pude realizar también en local).
- Componentes esenciales: Entre los datos y documentos que se debe proteger se encuentran listas, inventarios, copias de seguridad de software y datos, cualquier otra lista importante de materiales y documentación. La creación previa de plantillas de verificación ayuda a simplificar este proceso.
  Un resumen del plan debe ser respaldado por la gerencia. Este documento organiza los procedimientos, identifica las etapas importantes, elimina redundancias y define el plan de trabajo. La persona o personas que escriban el plan deben detallar cada procedimiento, tomando en consideración el mantenimiento y la actualización del plan a medida de que el negocio evoluciona. El plan asigna responsabilidad a diferentes equipos / departamentos y alternos.
- Criterios y procedimientos de prueba del plan: La experiencia indica que los planes de recuperación deben ser probados en su totalidad por lo menos una vez al año. La documentación debe especificar los procedimientos y la frecuencia con que se realizan las pruebas. Las razones principales para probar el plan son: verificar la validez y funcionalidad del plan, determinar la compatibilidad de los procedimientos e instalaciones, identificar áreas que necesiten cambios, entrenar a los empleados y demostrar la habilidad de la organización de recuperarse de un desastre.
  Después de las pruebas el plan debe ser actualizado. Se sugiere que la prueba original se realice en horas que minimicen trastornos en las operaciones. Una vez demostrada la funcionalidad del plan, se debe hacer pruebas adicionales donde todos los empleados tengan acceso virtual y remoto a estas posiciones y funciones en el caso de un desastre. Antes de las pruebas totales, y para evitar impactos no previstos, se deben realizar otro tipo de pruebas, desde revisión de la documentación por el personal, crear escenarios simulados donde cada responsable comunica los pasos a realizar y se valida contra una serie de pasos predefinidos correctos, o bien pruebas parciales reales.
- Aprobación final: Después de que el plan haya sido puesto a prueba y corregido, la gerencia deberá aprobarlo. Ellos son los encargados de establecer las pólizas, los procedimientos y responsabilidades en caso de contingencia, y de actualizar y dar el visto al plan anualmente. A la vez, sería recomendable evaluar los planes de contingencia de proveedores externos.

A continuación se adjunta la guía INCIBE para el desarrollo de planes de continuidad y contingencia en español, plantilla de un plan de continuidad de negocio (PCN) en inglés y una plantilla de un plan de recuperación TI ante desastres, también en inglés.

Gestión de incidentes

Un incidente de seguridad es cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

Tipologías (de acuerdo al Instituto Nacional de Ciberseguridad):

- Ataques: Dirigido // Defacement.
- Código malicioso: Infección extendida // Única.
- DoS/DDoS: Exitoso: No exitoso.
- Acceso no autorizado, robo o pérdida de equipos y de datos.
- Pruebas y reconocimientos: Pruebas no autorizadas // Alarmas sistemas monitorización.

- Daños o cambios físicos no autorizados a los sistemas.
- Abuso de privilegios y usos inadecuado: Abuso de privilegios o de políticas de seguridad // Infracciones de derechos de autor // Uso indebido de la marca.

A continuación se muestra el enlace a la guía de incidentes en detalle en español: https://www.incibe.es/protege-tu-empresa/blog/incidentes-seguridad-conoce-tus-enemigos

La gestión de incidentes de seguridad es el conjunto de procesos en una organización para la gestión de un incidente de seguridad a lo largo de todo su ciclo de vida, así como una serie de actividades relacionadas para asegurar la mejora continua de dichos procesos.
Estos procesos deben plasmarse en un Plan de Gestión de Incidentes, documento que recoge la categorización de incidentes, pasos a dar de forma general, los pasos específicos por tipo de incidente, roles y responsabilidades, tiempos de respuesta de cada paso, procedimientos de notificación, escalado y declaración de un incidente, etc.

Los pasos a tomar, de forma general, son los siguientes:

Los pasos a tomar parecen secuenciales, con un ciclo desde las actividades post-incidente al inicio, preparación, para la adecuación del plan tras incidentes concretos. Sin embargo, dentro de un incidente puede ser necesario volver varios pasos atrás según se recopila más información (por ejemplo, volver a recategorizar un incidente en la etapa de contención).

A continuación se muestran los enlaces con mayor detalle de varios aspectos:

- Guía INCIBE para la categorización de incidentes de seguridad.
- Plantilla de gestión de incidentes (inglés).
- Ejemplo de planes de respuesta a incidentes público (en inglés).
- Más información en español sobre el modelo de gestión de incidentes.

Fase 1: Preparación

Esta etapa dentro del ciclo de vida de respuesta a incidentes suele hacerse pensando no sólo en crear un modelo que permita a la entidad estar en capacidad de responder ante estos, sino también en la forma como pueden ser detectados,
evaluados y gestionar las vulnerabilidades para prevenirse, asegurando que los sistemas, redes, y aplicaciones son lo suficientemente seguros.

En esta etapa el grupo de gestión de incidentes o quien se designe para esta labor debe velar por la disposición de los recursos de atención de incidentes y las herramientas necesarias para cubrir las demás etapas del ciclo de vida del mismo, creando (si no existen) y validando (si existen) los procedimientos necesarios y programas de capacitación.

También se deben preparar aspectos como los procedimientos y recursos para comunicación (interna y externa, como por ejemplo con fuerzas de seguridad, prensa, etc), hardware y software necesario, etc.

Fase 2: Detección y análisis

Los indicadores son los eventos que nos señalan que posiblemente un incidente ha ocurrido generalmente algunos de estos elementos son:

- Alertas en sistemas de seguridad.
- Caídas de servidores.
- Reportes de usuarios.
- Software antivirus dando informes.
- Otros funcionamientos fuera de lo normal del sistema.
  Una vez detectado por cualquiera de los medios (reporte de usuario, alerta en un SIEM, etc), se debe hacer un análisis inicial del incidente recopilando información básica que permita descartar falsos positivos y priorizar. Se debe recopilar información como:
- Cuándo ocurrió?
- Cómo se descubrió?
- Quién lo descubrió?
- Han sido impactadas otras áreas?
- Cuál es el alcance del compromiso?
- Afecta a las operaciones?
- Se ha descubierto el punto de entrada/origen?

Finalmente, en caso de no ser descartado como un falso positivo, se debe priorizar de acuerdo a su criticidad y el impacto en la organización y asignar a un gestor de incidentes cualificado (generalmente en base a su tipología y los conocimientos necesarios para su gestión; no es lo mismo un ransomware que una exfiltración de información).

Fase 3: Contención, erradicación y recuperación

Es importante para la organización implementar una estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad
disponibilidad de la información, así como a la propia imagen de la organización.

Contención: esta actividad busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI, para facilitar esta tarea la entidad debe poseer una estrategia de contención previamente definida para poder tomar decisiones por ejemplo: apagar sistema, desconectar red, deshabilitar servicios. La estrategia de contención varía según el tipo de incidente y los criterios deben
estar bien documentados para facilitar la rápida y eficaz toma de decisiones. Algunos criterios que pueden ser tomados como base son:

- Criterios Forenses.
- Daño potencial y hurto de activos.
- Necesidades para la preservación de evidencia.
- Disponibilidad del servicio.
- Tiempo y recursos para implementar la estrategia.
- Efectividad de la estrategia para contener el incidente (parcial o total).
- Duración de la solución.

Erradicación y Recuperación: Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el administrador de TI o quien haga sus veces deben restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro. Las estrategias de erradicación son muy diversas, como instalar un parche de seguridad, cambiar la configuración de sistemas, etc. Para la recuperación se pueden tener también varias estrategias, como recuperar información dañada desde una copia de seguridad, reinstalar un sistema desde cero, etc.

Fase 4: Actividades post-incidente

Las actividades Post-Incidente básicamente se componen del reporte apropiado del Incidente, la generación de lecciones aprendidas, el establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias así como el
registro en la base de conocimiento para alimentar los indicadores (IoC o Indicadores de Compromiso, reglas que permitirán en el futuro detectar el mismo incidente de forma más rápida y automatizada en IDS, SIEM, etc).

Una de las partes más importantes de un plan de respuesta a incidentes es la de aprender y mejorar. Cada equipo de respuesta a incidentes debe evolucionar para reflejar las nuevas amenazas, la mejora de la tecnología, y las lecciones
aprendidas. Mantener un proceso de “lecciones aprendidas” después de un incidente grave, y periódicamente después de los incidentes menores, es sumamente útil en la mejora de las medidas de seguridad y el proceso de gestión de incidentes. Mantener un adecuado registro de lecciones aprendidas permite conocer:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
    - Los procedimientos documentados.
    - Si se tomaron las medidas o acciones que podrían haber impedido la recuperación.
    - Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.
    - Acciones correctivas pueden prevenir incidentes similares en el futuro.
    - Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

El proceso de lecciones aprendidas puede poner de manifiesto la falta de un paso o una inexactitud en un procedimiento y son un punto de partida para el cambio, y es precisamente debido a la naturaleza cambiante de la tecnología de la información y los cambios en el personal, que el equipo de respuesta a incidentes debe revisar toda la documentación y los procedimientos para el manejo de incidentes en determinados intervalos. Es por ello además que esta fase enlaza con la primera de Preparación, dado que con estas actividades debe comenzar el proceso de nuevo mejorando los documentos, procesos, procedimientos, herramientas, etc.

Monitorización del riesgo

Riesgo, monitorización y reporte

La monitorización continua y el reporte del riesgo es un proceso dinámico que requiere una participación a nivel global. Para ser efectiva, la función de gestión del riesgo (como el comité de riesgo y el responsable del riesgo) deben tratar las tendencia clave antes de que se conviertan en problemas (como las desviaciones) y ser reportadas de forma periódica a los stakeholders clave.

El reporte del riesgo es el proceso de comunicación los riesgos en tiempo real (para los críticos), o de forma regular (con tiempos definidos en el marco de gestión del riesgo) y el rendimiento a los diferentes stakeholders.

La monitorización del riesgo es una actividad continua que permite la concienciación de qué está sucediendo actualmente en diferentes partes de la organización.

De forma estratégica, a lo largo del tiempo, la monitorización del riesgo permite a la gerencia:

- Identificar tendencias críticas.
- Responder de forma apropiada y eficiente.
- Descubrir oportunidades de negocio o mejoras en procesos que de otra forma no serían aparentes sin una correcta monitorización.

Esto se pude lograr mediante diferentes técnicas:

- Los mapas de riesgo y el perfil de riesgo se pueden generar en cualquier momento y ser compartidos con diferentes stakeholder como medio de reporte.
- Los resultados de pruebas y los valores de aseguramiento se pueden obtener mediante agregación desde el registro del riesgo hasta la evaluación del riesgo estratégico para el reporte estratégico, proveyendo la capacidad de ver el riesgo en un cuadro de mandos.
- Las métricas pueden ser enlazadas a los riesgos para seguir y monitorizar el riesgo y diferentes disparadores o alarmas se pueden utilizar en combinación con las métricas para notificar a los stakeholders y conducir la toma de decisiones en tiempo real.
- Los informes de seguimiento y desviaciones, así como todas las evaluaciones del riesgo (totales o parciales) se pueden enlazar con los diferentes indicadores y métricas para facilitar la detección de problemas potenciales y facilitar la toma de decisiones sobre las estrategias de tratamiento y correcciones sobre las mismas.

El aseguramiento del riesgo puede ser reportado a nivel agregado o granular, dependiendo de las necesidades de la audiencia a las que se dirijan (p.e capas 1, 2 o 3).

El riesgo debe ser monitorizado continuamente y de forma automática para integrar los datos de métricas de resultados, permitiendo a la gerencia y al comité de dirección realizar decisiones más rápidas y con el riesgo cuantificado.

A nivel más operativo, la monitorización del riesgo provee a las organizaciones de formas de:

- Validar el cumplimiento legal, regulatorio y contractual.
- Determinar la efectividad continua de las medidas de respuesta al riesgo.
- Identificar los cambios que impactarían al riesgo sobre SI y entornos de operación.

Analizar los resultados de la monitorización da a las organizaciones la capacidad de mantener la concienciación sobre el riesgo incurrido, destacar la necesidad de revisitar otros pasos en el proceso de gestión del riesgo e iniciar actividades de mejora del proceso según sean requeridas.

Las organizaciones pueden establecer la monitorización en cualquiera de las capas de gestión.

- Las actividades de monitorización en capa 1 pueden incluir evaluaciones del riesgo continuas y cómo los cambios en el espacio del riesgo pueden afectar a las actividades de la capa 2 y 3.
- Las actividades a nivel de capa 2 podrían incluir el análisis de tecnologías nuevas o existentes para identificar debilidades explotables y/o deficiencias que podrían afectar al éxito del negocio.
- En la capa 3, las actividades se centran en los SI y podría incluir, por ejemplo, la monitorización automática de los valores de configuración estándar de los productos TI, escaneo de vulnerabilidades y valoraciones continuas de los controles de seguridad.

Además de decidir sobre las actividades necesarias de monitorización a través de las capas de gestión del riesgo, las organizaciones también deben decidir sobre cómo se realizara la monitorización (p.e si automatizada o manual, dado que no todas las mediciones se pueden automatizar) y la frecuencia de dichas mediciones basado, por ejemplo, en la frecuencia en que los controles de seguridad desplegados cambian, los elementos críticos sobre los planes de acción y los hitos y la tolerancia al riesgo.

Requisitos para la monitorización del riesgo

Las entradas para este proceso incluyen las estrategias de implementación de las respuestas al riesgo y la implementación actual de los cursos de acción seleccionados. Así mismo, el proceso puede recibir información desde el marco de gestión del riesgo (p.e cuando las organizaciones descubren una amenaza avanzada persistente, APT, que refleje un cambio en las asunciones sobre el riesgo, esto podría resultar en un cambio en la frecuencia de las actividades de monitorización). El marco también da forma a las restricciones de recursos asociadas con el establecimiento e implementación de la estrategia global de monitorización.

En algunos casos, las salidas de la evaluación del riesgo pueden ser entradas útiles para este proceso. Por ejemplo, las condiciones umbral de evaluación del riesgo (p.e las probabilidades de las amenazas explotando las vulnerabilidades). A su vez, las organizaciones podrían monitorizar si estas condiciones umbral han sido alcanzadas, Si sucede así, esta información debería ser utilizada en la evaluación del riesgo, sirviendo como base para una evaluación del riesgo diferencial o una re-evaluación total del riesgo de la organización.

Actividades para la monitorización y reporte del riesgo

En esta sección se muestra de forma breve los pasos a realizar, centrándonos más en el “qué” que en el “cómo”. Para más información sobre el proceso, se puede consultar la sección correspondiente del estándar NIST 800-39 “Managing information security risk“.

Desarrollar una estrategia de monitorización para la organización que incluya el propósito, el tipo y al frecuencia de las actividades de monitorización

Las organizaciones implementan programas de monitorización del riesgo para:

- Verificar que las medidas de respuesta están implementadas y que los requisitos de seguridad de la información derivados de y trazables a los objetivos del negocio, leyes y regulaciones, directivas, políticas y estándares se satisfacen (**monitorización del cumplimiento**).
- Determinar la efectividad continua de las medidas de respuesta al riesgo tras su implementación (**monitorización de efectividad**).
- Identificar cambios de los SI y entornos de la organización en los cuales los sistemas operan que puedan afectar al riesgo (**monitorización del cambio**).

Determinar el propósito de los programas de monitorización del riesgo impacta de forma directa en los medios utilizados por la organización para realizar dichas actividades y dónde se realiza la monitorización (p.e. en qué capas de la gestión del riesgo).

Las organizaciones también determinan el tipo de monitorización a utilizar, incluyendo aproximaciones que dependen en la automatización o en actividades manuales/procedimentales con intervención humana, equilibrando el valor ganado de la monitorización frecuente contra el potencial de disrupción operacional debido a interrupción de procesos de negocio, reducción del ancho de banda operacional durante la monitorización y el cambio de recursos de operación a monitorización, por ejemplo.

Las estrategias de monitorización desarrolladas en la capa 1 influencian y proveen de dirección a las estrategias similares desarrolladas en las capas 2 y 3, incluyendo las actividades de monitorización asociadas con el marco de gestión del riesgo al nivel de SI.

Monitorización de los SI y entornos de operación de la organización de manera continuada para verificar el cumplimiento, determinar la efectividad de las respuestas e identificar cambios

Una vez se han desarrollado las estrategias de monitorización, estas deben ser implementadas a nivel organizacional. Dado que existen tantos aspectos en la monitorización, no todos serán realizados, o pueden ser realizados en momentos diferentes.

Los aspectos particulares que serán ejecutados serán dictados principalmente por las asunciones, restricciones, tolerancia al riesgo y prioridades establecidas por las organizaciones en el establecimiento del marco de gestión del riesgo. Por ejemplo, si bien las organizaciones querrían realizar todas las formas de monitorización, las restricciones establecidas podrían permitir la monitorización del cumplimiento que pueda ser fácilmente automatizada en la capa 3. Si se pueden soportar diferentes aspectos de la monitorización, la salida del marco ayuda a las organizaciones a determinar el grado de énfasis y nivel de esfuerzo a utilizar en las diferentes actividades. Como se ha comentado, no todas las actividades son realizadas en las mismas capas, para los mismos propósitos o utilizando las mismas técnicas. Sin embargo, es importante que la organización intente coordinar las diferentes actividades de monitorización.

Esta coordinación facilita la compartición de información relacionada con el riesgo, que podría ser útil para proveer de una alerta temprana, desarrollar información de tendencias o asignar medidas de respuesta al riesgo de forma eficiente y oportuna. Si la monitorización no está coordinada, el beneficio de las diferentes actividades se reduciría, y podría socavar el esfuerzo global para identificar y tratar el riesgo.

Los resultados de la monitorización se aplicarán en la realización de evaluaciones del riesgo incrementales para mantener el conocimiento del riesgo incurrido, para destacar los cambios en el riesgo y para indicar la necesidad de revisitar otros pasos del proceso de gestión del riesgo cuando sea necesario.

Comunicación del riesgo

La comunicación del riesgo es una parte integral del proceso de evaluación y en general de la monitorización y reporte de la gestión del riesgo (dado que se trata de un proceso continuo), que implica los procesos de comunicación entre los diferentes roles y responsabilidades (vistos anteriormente).

El proceso de comunicación se debe diseñar para ser iterativo (p.e tras nuevas re-evaluaciones del riesgo) y para informar de las decisiones de evaluación y gestión.

El objetivo es que todos los stakeholders (desde el comité de dirección a los responsables de áreas / servicios / procesos e incluyendo a terceros externos como organismos de control regulatorio) tengan una comprensión común de los procesos y asunciones realizados,

El nivel y tipo de comunicación varía dependiendo de la complejidad de la organización (p.e centralizadas vs hibridas) y el nivel de riesgo potencial y la percepción del mismo por las partes.

Algunos aspectos críticos que se deben tener en cuenta son los siguientes.

Solicitar información a los stakeholders

La comunicación con los stakeholders debe ser iterativa y soportar todas las fase de la evaluación y gestión del riesgo, desde la definición del alcance a la implantación de salvaguardas u otras opciones de tratamiento.

La involucración temprana y sincera de los stakeholders a menudo mejora la calidad del trabajo realizado, a la vez que acelera y facilita el proceso de revisión.

Reconocer los retos en la percepción e interpretación del riesgo

Incluso aunque los diferentes stakehodlers deberían estar familiarizados con el proceso de gestión del riesgo (p.e mediante el marco de gestión del riesgo y su comunicación a todas las partes), estos a menudo tienen diferentes perspectivas sobre la importancia de los hallazgos en la evaluación y las acciones de tratamiento apropiadas. Así, estas diferentes perspectivas afectan la percepción de los riesgos por los stakeholders.

La percepción del riesgo involucra la influencia de factores subjetivos sobre cómo los riesgos se comprenden y valoran. Las características de una amenaza y el contexto subjetivo del receptor (vistas personales cualitativas) son tan importantes como el riesgo cuantificado objetivo en la influencia de la percepción de un individuo del riesgo.

Por ello, la comunicación del riesgo no debe infraestimar la importancia y validez de la percepción.

Pasos para la comunicación y compartición de los resultados de la evaluación del riesgo

1. Comunicar los resultados a los decisores para la toma de decisiones. Las organizaciones pueden comunicar los resultados de varias formas (p.e sesiones informativas ejecutivas, informes de evaluación del riesgo, cuadros de mando, etc). Estas pueden ser formales o informales con el contenido y formato definido por la organización, debiendo esta proveer guía sobre la comunicación de riesgos específicos y los requisitos de reporte como parte de la preparación de la evaluación (en caso de no estar incluido en el marco de gestión del riesgo).
2. Compartir la información relacionada con el riesgo producida durante la evaluación con el personal adecuado. Las organizaciones comparten información de origen y los resultados intermedios, y proveen de guía sobre la compartición de la información relacionada. Esto ocurre principalmente mediante informes y sesiones informativas, así como mediante la actualización de los repositorios de datos de riesgos (p.e. el registro del riesgo) con información que de soporte a los resultados. La compartición se soporta también mediante la documentación de las fuentes de información, los procesos analíticos y los resultados intermedios, de forma que las evaluaciones pueden ser mantenidas de forma sencilla.

KRIs (Indicadores Clave del Riesgo)

Estos indicadores son métricas que miden la probabilidad de que ocurra un riesgo. Un indicador de riesgo es un elemento cuyos valores se calculan con base en datos históricos. De esa manera se representan los factores de riesgo a los cuales se expone una compañía.

El uso de indicadores es importante porque permite tener una visión multidimensional del perfil de riesgo, además de que son dinámicos y ayudan a validar el marco de gestión.

Estos indicadores:

- Sirven como herramienta de monitorización y mitigación de los riesgos.
- Avisan cuando algo no funciona como debería.
- Ofrecen una alerta temprana a los gerentes para que tomen las acciones oportunas.
- Identifican la exposición actual al riesgo y las tendencias de riesgo emergentes.
- Subrayan las debilidades de los controles.
- Ayudan a fortalecer los controles deficientes.
- Facilitan el proceso de informe y escalado de riesgos.

- Validan y mejoran el marco de evaluación de riesgos.
- Pueden usarse en procesos de benchmarking (comparativa, por ejemplo entre áreas/procesos/servicios o contra otras organizaciones).

Para que estos indicadores sean efectivos, deben cumplir los siguientes requisitos:

- Medibles: deben ser cuantificables (en número, porcentaje, volumen, etc).
- Predictivos: deben generar alertas tempranas.
- Comparables: deben mostrar una evolución en el tiempo.
- Informativos: deben promocionar datos útiles para tomar decisiones.

Estos KRIs pueden ser divididos en diferentes tipologías:

- Causales: Indicadores que miden las causas de los riesgos (p.e % de tiempo de caída de sistemas crítico).
- Efectividad de los controles: Cómo de bien está funcionando un control o salvaguarda (p.e % de incidentes detectados por tipología en un tiempo dado // tiempo de despliegue de parches por criticidad y tipología de sistema/dispositivo // tiempo de corrección de vulnerabilidades por criticidad).
- Volumen: Indicadores que miden volumen de situaciones o datos cuya variación afecta los riesgos (p.e número de incidentes de seguridad por tipología // número de vulnerabilidad de aplicaciones o sistemas por criticidad).

En el diseño de los indicadores se deben tomar en cuenta varios aspectos:

- Fuentes de las que se medirán: Si son automáticas (como herramientas) o manuales (como informes). También el cómo se recopilará la información de dichas fuentes (introducción manual, uso de APIs para alimentar una herramienta, etc).
- Establecimiento de umbrales de alerta y alarma, lo que permitirá actuar antes de que un indicador llegue a un valor crítico que impacte a la organización.
- Proceso de mejora y madurez: Según la organización madura en su proceso de seguridad, se deberán crear nuevas métricas o actualizar las existentes, todo ello con el objetivo de reflejar las necesidades en cada momento.

En este proceso es conveniente ser muy prudente y no intentar medir todo al mismo tiempo. Dependiendo del nivel de madurez de la organización puede ser necesario comenzar con unos pocos indicadores básicos y de alto nivel, y desde ahí comenzar a madurar dichos indicadores según maduran a la vez los procesos de seguridad de la información.

A continuación se muestran una serie de indicadores típicos (ejemplo, no una lista exhaustiva) que pueden ser utilizado, si bien se recomienda que el conjunto concreto sea diseñado específicamente para la organización y su nivel de madurez (no existen recetas mágicas por desgracia):

- Métricas de amenazas: Las métricas del nivel de amenazas buscan medir cómo de expuesta está la organización a las amenazas de seguridad. Este riesgo puede ser externo o interno.
    - Riesgo externo:
        - El número de incidentes de seguridad reportados por otras firmas en los últimos X meses.
        - El volumen de peticiones/tráfico originado desde direcciones IP maliciosas o desconocidas.
        - El volumen de intentos de ingeniería social reportados en la organización en los últimos X meses.
    - Riesgo interno:
        - Número de amenazas de vulnerabilidad recibidas desde proveedores o herramientas de escaneo en los últimos X meses.
        - El % de controles TI que han sido certificados como funcionando correctamente.
        - % de parches aplicados por criticidad y tipología de dispositivo.
- Métricas de nivel de riesgo: Mide la posición actual de la organización respecto de sus riesgos. (Para esto se necesita disponer de un registro del riesgo como se ha hablado anteriormente).

    - % de incremento en el riesgo agregado residual.
    - La valoración del peor caso actual.
    - Número de evaluaciones del riesgo con resultados dentro del umbral de tolerancia.
- Nivel de cumplimiento: Cómo de bien está la organización cumpliendo con las obligaciones legales, regulatorias, de políticas y contractuales.
    - El % de empleados que han realizado y aprobado formación en ciberseguridad.
    - El % de controles TI que han sido certificados como funcionando efectivamente.
    - El % de controles de cada legislación/regulación con las que la organización debe cumplir que están cubiertos actualmente.
    - Número de desviaciones detectadas sobre las políticas de seguridad.
    - Número de excepciones aprobadas sobre las políticas de seguridad.
    - Número de hallazgos de auditorías abiertos.
    - % de cuentas de usuarios que cumplen con los requisitos de la organización (flujo de petición/modificación/eliminación, fortaleza de contraseñas, factores de autenticación, etc).
    - % de cuentas privilegiadas monitorizadas (la actividad realizada)
- Nivel de incidentes de seguridad: El análisis de los incidentes de seguridad a menudo provee a los stakeholders de negocio con una perspectiva adicional sobre los riesgos permitiendo reevaluar los valores de riesgo actuales.
    - Número de incidentes por tipología (malware, exfiltración de información, phishing, etc).
    - Número de brechas de seguridad.
    - Número de intentos de phishing reportados.
    - % de fuentes de eventos de seguridad monitorizadas.
- Ejecución de proyectos de ciberseguridad: Por lo general las organizaciones suelen tener una serie de proyectos de mejora de la ciberseguridad en marcha y que son críticos para la gestión del riesgo. Por ello es importante el seguimiento de esta información.
    - % ejecutado vs proyectado por cada proyecto.
    - Retraso medio y peor retraso en los proyectos.
- Formación y concienciación: Cómo de concienciado está el personal y conoce sus responsabilidades respecto de la seguridad de la información.
    - % personal que ha pasado los cuestionarios asociados a las formaciones a la primera.
    - % de personal de TI/seguridad que ha recibido formación específica.
    - Número de campañas de concienciación ejecutadas (correos, posters, etc).

Herramientas para monitorización del riesgo.

Existen una serie de técnicas que permiten hacer un seguimiento del riesgo y por tanto monitorizarlo:

- Reevaluaciones del riesgo: Tanto de forma total como parcial o incremental, se deberían realizar nuevos análisis para validar el nivel de riesgo actual por áreas/servicios/procesos. Si bien los análisis de riesgos suelen realizarse cada 2 años (dependiendo de la organización) o tras cambios con un gran impacto, los análisis incrementales o bien parciales sobre ciertas áreas/servicios/procesos permitirán actualizar el nivel de riesgo de la organización e incluir en el riesgo presente las nuevas medidas implementadas/mejoradas.
- Auditorías del riesgo: Examinar y documentar la efectividad de la planificación de la respuesta al riesgo para el control del riesgo y la efectividad de los propietarios del riesgo.
- Análisis de varianza y tendencia: Las desviaciones significativas indican que se debería realizar una identificación y análisis de riesgos actualizada.
- Reuniones de seguimiento: Si bien esto es un trabajo bastante manual y la interpretación de los resultados compleja, es una herramienta muy poderosa de cara a evaluar aspectos más subjetivos de le gestión del riesgo, incluyendo el clima respecto al proceso.

Así mismo, existen una serie de herramientas que facilitarán ejecutar la monitorización:

- Registro del riesgo: Como repositorio central de todos los riesgos y el estado del mismo, será la pieza central de cara a obtener el estado en cada momento. Dependiendo de si se trata de una herramienta simple

(como un excel) o una herramienta específica, se podrán además generar informes con la información contenida (por áreas, periodos temporales, tipologías de riesgos, etc).

- Herramientas GRC (Gobierno, Riesgo y Cumplimiento): El software de GRC permite a las organizaciones integrar y gestionar las operaciones de TI que están sujetas a regulación. Asimismo, permite adoptar un enfoque sistemático y organizado para la gestión e implementación de estrategias relacionadas con GRC. En lugar de guardar los datos en diferentes "silos", los administradores pueden utilizar un marco único para monitorizar y hacer cumplir las reglas y procedimientos (incluyendo por ejemplo un registro del riesgo). Las instalaciones exitosas permiten a las organizaciones gestionar el riesgo, reducir los costos causados por varias instalaciones y minimizar la complejidad para los administradores. La implementación de este tipo de aplicaciones normalmente implica instalaciones complejas, que incluyen la coordinación de los datos entre múltiples departamentos, incluyendo negocios, TI, seguridad, cumplimiento y auditoría. Una vez instalado, sin embargo, los cuadros de mando y las herramientas de análisis de datos permiten a los responsables identificar la exposición al riesgo de la organización, medir el progreso hacia las metas trimestrales o rápidamente reunir una auditoría de la información. Se puede pensar en GRC como el enfoque que va a permitir alinear los objetivos de negocio con los riesgos derivados de la actividad y el cumplimiento de los requisitos legales y normativos.

Estas herramientas generalmente se aplican a nivel corporativo para diferentes funciones, no sólo seguridad, siendo bastante complejas. Desde el punto de vista de la seguridad (bien dentro de una herramienta GRC general o en una aplicación específica para seguridad de la información), una herramienta de este tipo debería permitir:

  - Realizar un modelado de activos y su valoración.
  - Permitir el análisis y gestión de riesgos (cuantitativo y cualitativo, con plantillas de valoración).
  - Permitir el análisis del cumplimiento legal y regulatorio.
  - Gestión de la continuidad de negocio.
  - Disponer de un catálogo modificable en base a estándares y mejores prácticas de activos, amenazas, vulnerabilidades y salvaguardas.
  - Disponer de plantillas documentales y repositorio documental para la gestión de seguridad y cumplimiento (SGSI, continuidad de negocio, RGPD, etc).
  - Permitir la gestión de empresas complejas creando diferentes capas a la vez que unidades de negocio y/o la gestión multiempresa (para grupos empresariales).
  - Proporcional métricas y capacidad de monitorización y reporte de seguridad y de la gestión del riesgo.
- SIEM: Las herramientas de monitorización de información y eventos de seguridad, además de servir para detectar posibles incidentes de seguridad, gracias a integrar múltiples fuentes de seguridad y disponer de catálogos de informes y cuadros de mando para cumplimiento y gestión del riesgo permitirán realizar una monitorización de ciertos aspectos más técnicos (como sistemas con vulnerabilidades, infecciones por malware, etc).

- Plantillas excel (o sistemas similares): Si bien resulta un elemento muy poco tecnológico, dado que es imposible automatizar el análisis y lectura de toda la información necesaria, en muchos casos será necesario crear plantillas para poder introducir la información necesaria dentro de otras herramientas de gestión y monitorización del riesgo.

Otro tipo de herramientas para la gestión TI generalista, pero que serán fundamentales para la monitorización del riesgo de seguridad son las siguientes:

- CMDB: Una base de datos de la gestión de configuración (CMDB, por sus siglas en inglés) es una base de datos que contiene detalles relevantes de cada CI (ítem/elemento de configuración) y de la relación entre ellos, incluyendo el equipo físico, software y la relación entre incidencias, problemas, cambios y otros datos del servicio de TI. La CMDB es un repositorio de información donde se relacionan todos los componentes de un sistema de información, ya sean hardware, software, documentación, etc. Esta herramienta facilitará la evaluación de riesgos toda vez que la identificación de activos ya ha sido realizada y se dispone del catálogo centralizado.
- Herramientas de descubrimiento de activos: Estas herramientas, de forma pasiva o activa, permiten descubrir diferentes activos así como información sobre los mismos, pudiendo en algunos casos integrarla directamente en la CMDB.
- Herramientas de monitorización de salud: Estas herramientas permiten monitorizar el estado de los servidores, aplicaciones, dispositivos de red, BBDD, etc desde el punto de vista de la salud (uso de memoria, cortes en comunicación, procesos funcionando, etc). lo que permitirá una gestión más afectiva de la disponibilidad (estableciendo a la vez umbrales de aviso y análisis de tendencias).

Por otro lado, se debe tener en cuenta que se debería integrar, en la medida de los posible, las diferentes herramientas de ciberseguridad (gestión de vulnerabilidades, DLP, EDR, protección de BBDD, etc) con las herramientas de monitorización del riesgo con el objeto de disponer de una imagen actualizada y completa de la organización.