sedian

Seguridad Digital
de Andalucía

Medidas de contención, mitigación y recuperación, así como protocolo para recolección y custodia de evidencias una vez que hemos detectado un ciberincidente

Sesión 1: 15 de marzo de 2021

Junta de Andalucía

INDICE

Medidas de Seguridad

Medidas de Seguridad

- **¿Qué es una medidas de seguridad?**

Ante de empezar a hablar de cualquier tipo de medida de seguridad tenemos que entender que es una medida de seguridad:

"Una medida de seguridad o salvaguarda o defensa o control o contramedida, es cualquier medio empleado para reducir el riesgo de una amenaza."

Una medida de seguridad puede incluir políticas, procedimientos, directrices, prácticas o estructuras de la organización, y que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Como ejemplos de medidas de seguridad tenemos:	La autenticación de usuarios
	El control de accesos.
	El cifrado
	FireWall
	IDS.
	Etc.

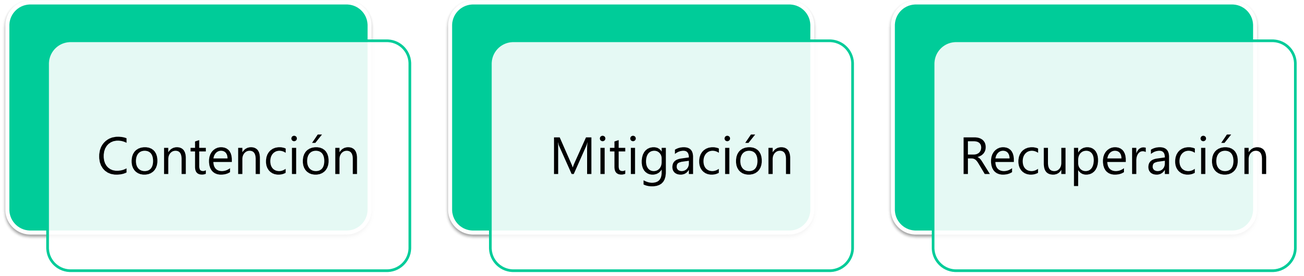
También son medidas de seguridad:	Políticas de seguridad
	Procedimientos de seguridad.
	Normativas de seguridad.
	Formación.
	Concienciación.
	Etc.

Medidas de Seguridad

- **¿Qué tipos de medidas de seguridad existen?**

Existe una gran de variedad de clasificaciones de medidas de seguridad, desde las que nos enumeran las distintas metodologías, hasta las propias que nosotros podemos definir.

Para hablar de todas las clasificaciones de seguridad necesitaríamos disponer de un montón de horas. A día de hoy nos vamos a centrar en las que son objeto de estudio de este curso:



Medidas de Seguridad

- **Introducción**

Una Organización, tanto pública como privada, deben llevar una gestión adecuada de las medidas de seguridad. Deben elegir las medidas de seguridad más adecuadas para cada amenaza y cada activo. Se debe gestionar con mucho detalle su proceso de implantación, se debe verificar que la medida elegida sea eficaz, medir sus resultados, si son los esperados o no, si necesita complementarse con otra medida de seguridad, etc.

Cuando empezamos el proceso de selección de medidas de seguridad , podemos encontrarnos que no es sencillo y para ayudarnos siempre es recomendable apoyarnos en alguna metodología que ya nos presente un catalogo de medidas donde podamos elegir.

El ANEXO del Esquema Nacional de Seguridad, el Anexo de la ISO 27001, NIST 800-53; o si buscamos algo más específico (Técnico) tenemos los controles de OWASP, PCI-DSS, COBIT, COSO, SOX, etc. Incluso cuando ya hayamos adquirido una madurez podemos definir nuestros propios controles.

Algo muy importante es que usemos lo que usemos debemos ir creado nuestro registro de medidas de seguridad, nuestra Declaración de Aplicabilidad, que no es más que un catalogo de todas las medidas de seguridad que hemos elegido para implantar y que debe contener toda la información posible de las mismas (Una descripción, una razón de porque las hemos elegido, el estado de madurez en el que se encuentran, etc.

Medidas de Seguridad

- **¿Cómo elegimos una medida de seguridad?**

En la vida real hay una gran tendencia a elegir un catálogo de medidas de seguridad y comenzar a implantarlas todas. Ya pueda ser por desconocimiento de la materia, falta de recursos, falta de tiempo, falta de concienciación o simplemente por decisiones de la Alta Dirección.

El proceso que se debe seguir para elegir una medida de seguridad es tremendamente complejo y no puede depender de una única persona. Para poder elegir adecuadamente una medida de seguridad primero debemos conocer muy bien el organismo a proteger, todos sus activos, recopilar toda la información sobre los mismos, saber a que amenazas está expuesto, etc. En resumen se debe hacer una **gestión de riesgos**.

Análisis de Riesgos

Análisis de riesgos

El concepto de Riesgo se encuentra presente en todos los ámbitos desde la salud, la ingeniería, la prevención, jurídica, etc. Es importante estudiar los riesgos de los proyectos, de las servicios, procesos, actividades, etc. Ya que un buen análisis de riesgos nos puede prevenir de una mala inversión, nos puede preparar para posibles incidentes o simplemente para mantener un nivel adecuado de seguridad en la empresa.

A día de hoy, el uso de las tecnologías de la información se ha intensificado drásticamente, tanto en el mundo doméstico como en el mundo empresarial (independiente de la naturaleza y actividad). Se encuentran en constante evolución adaptándose a las nuevas necesidades de los distintos organismos y así mismo dando lugar a nuevas necesidades relacionadas con su operativa diaria.

El rápido crecimiento de las tecnologías de la información y la importancia que han adquirido, las han convertido en blanco de ataques para los delincuentes. Los riesgos asociados a las empresas y a las propias tecnologías se intensifican y se transforman, por ello se hace necesario crear y adaptar constantemente los medios y métodos utilizados para mantener y actualizar la seguridad de la información de los organismos y de las personas.

Un riesgo puede afectar a las personas, a los servicios, a los procesos, metas y objetivos de las empresas y al mismo tiempo ser causa de otro tipo de riesgos al ser intrínseco al uso de tecnología. Por ello el daño (afectando a la integridad), la interrupción (afectando a la disponibilidad), o los accesos no autorizados (afectando a la confidencialidad) a las tecnologías de la información pueden implicar pérdidas significativas en las organizaciones, pérdidas financieras, multas o acciones legales, afectación de la imagen de una organización y causar inconvenientes a nivel operativo y estratégico.

Análisis de riesgos

- **El riesgo**

De una manera breve podemos definir la gestión del riesgos como el proceso por el cual una organización gestiona sus amenazas a niveles aceptables. Este proceso requiere el desarrollo e implementación de medidas de seguridad internas para gestionar y mitigar las amenazas en toda la organización, incluyendo los riesgos financieros, de inversión, el riesgo físico y el ciberriesgo.

- **El riesgo en la Ciberseguridad**

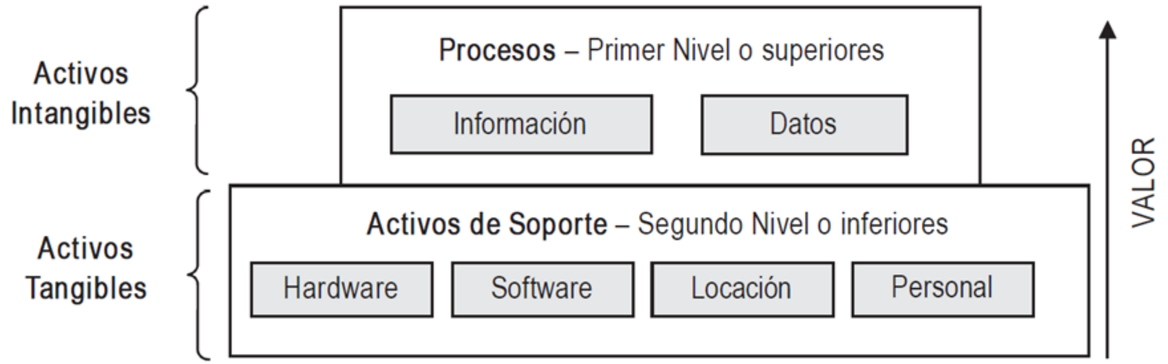
El deber principal de la ciberseguridad es identificar, mitigar y gestionar el riesgo de los activos de una organización. Podemos hablar de que existen tres enfoques diferentes para la implementación de la ciberseguridad:

Basado en cumplimientos:	• Este enfoque se basa en el uso de estándares para gestionar la seguridad (ISO 27001, ISO22301, NIST, PCI…), también se basa en el cumplimiento de reglamentos o normas para determinar las implementaciones de seguridad (LOPDGDD, GDPR, ENS, LPIC…).
Ad Hoc:	• Implementa la seguridad sin fundamento o criterio particular. Normalmente este criterio es el usado por empresas con un nivel de madurez entre 0-1, que están empezando y que por razones de desconocimiento, organizativas o económicas no pueden empezar el proceso de la gestión de la ciberseguridad.
Basado en riesgo:	• Se basa en identificar el riesgo al que una organización en particular se enfrenta y en diseñar e implementar los controles de seguridad para hacer frente a ese riesgo.

Análisis de riesgos

¿Cómo debemos enfocar la gestión del riesgo?

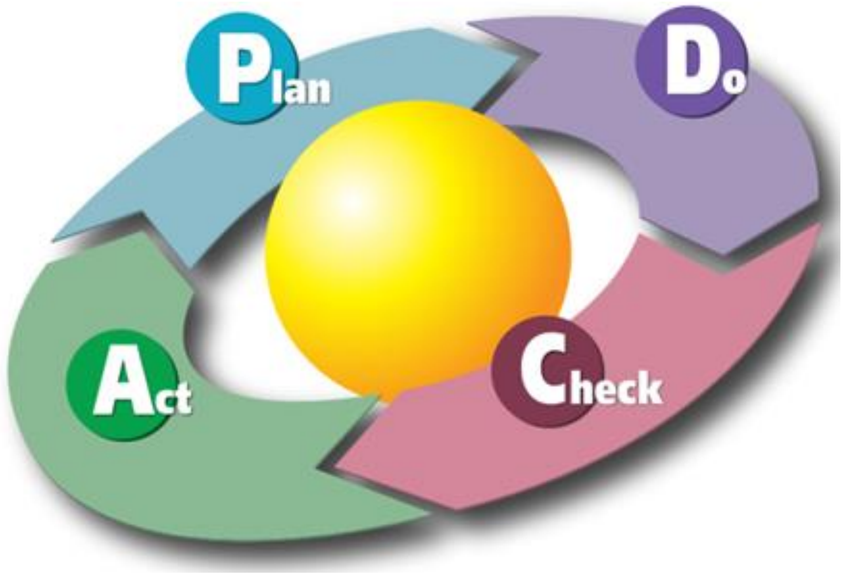
- En primer lugar, debemos enfocar la gestión del riesgo desde los activos intangibles, estos son los procesos fundamentales de los organismos. Este primer enfoque nos facilita el entendimiento (contexto interno y externo), la composición (direcciones, servicios, comités…), el funcionamiento de las actividades y procedimientos internos y externos del organismo.
- En segundo lugar debemos tener en cuenta los Activos Tangibles. Estos se relacionan, mantienen, con los activos intangibles analizados en el punto anterior. Se analiza hardware, software, servicios auxiliares recursos humanos y físicos, etc.
- **La finalidad de esta clasificación es centrar el estudio sobre los recursos críticos sin extenderse a activos irrelevantes.**



Análisis de riesgos

¿Cómo comenzamos a gestionar el riesgo?

- Aunque existen muchas y distintas metodologías nosotros vamos a ver en un principio las basadas en el Ciclo Deming o también conocido como el modelo Planificar-Hacer-Verificar-Actuar (Plan-Do-Check-Act). Todo para conseguir una metodología de riesgos integrada en un Sistema de Gestión.



Análisis de riesgos

¿Cómo comenzamos a gestionar el riesgo?

Planificar:

- En esta fase se establecen los objetivos, procesos y procedimientos para el proceso de gestión de riesgos tecnológicos. La finalidad de la planeación es la entrega de resultados acordes con las políticas y objetivos globales de la organización. Así mismo, se establece el plan de comunicaciones y el análisis del contexto organizacional actual para definir el alcance de la gestión de riesgos tecnológicos. En resumen, en esta fase se estudia la empresa y se desarrollan las políticas, normativas, procedimientos y toda la documentación.

Hacer:

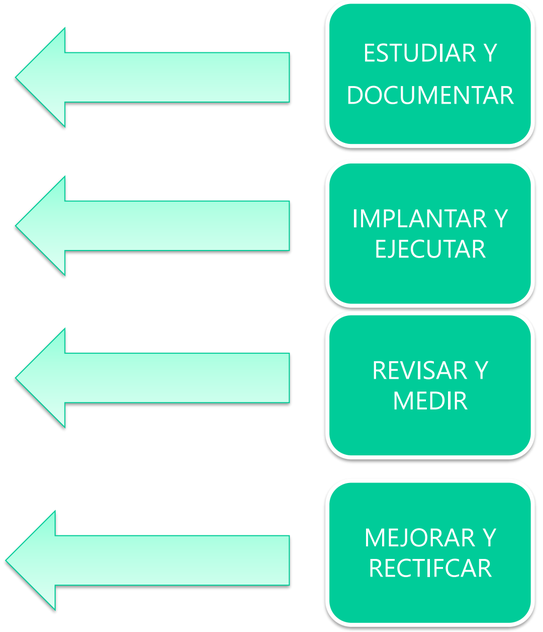
- En esta fase se procede a la implementación y operación de los controles, procesos y procedimientos (incluye la operación e implementación de las políticas definidas), lo correspondiente a la valoración y tratamiento de los riesgos.

Verificar:

- En esta fase se evaluar y medir el desempeño de los procesos contra la política de seguridad de la información y los objetivos de seguridad e informar sobre los resultados al Comité definido. En esta fase recopilamos toda la información para completar los indicadores definidos anteriormente y podemos valorar el estado del Sistema de Gestión.

Actuar:

- Establecer la política para la gestión de riesgos tecnológicos e implementar los cambios requeridos para la mejora de los procesos. Como parte de las fases verificar y actuar, se incluye la monitorización y mejora continua, donde se verifican los cambios y el cumplimiento de los indicadores que fueran establecidos desde la planificación. En este punto se desarrolla un nuevo plan de riesgos para mitigar o reducir los riesgos aún presentes, estudiar la madurez de los controles y poder tener un seguimiento del nivel de estado de los controles que se han decidido para gestionar los riesgos.



Análisis de riesgos

Proceso de gestión de riesgos

En primer lugar, debemos tener en cuenta:

- Ser una parte integrante de la gestión de la empresa.
- Estar integrado en la cultura y buenas prácticas.
- Deben encontrarse adaptado a los procesos de la empresa.

Todo el que pertenezca al organismo tiene una **responsabilidad**.

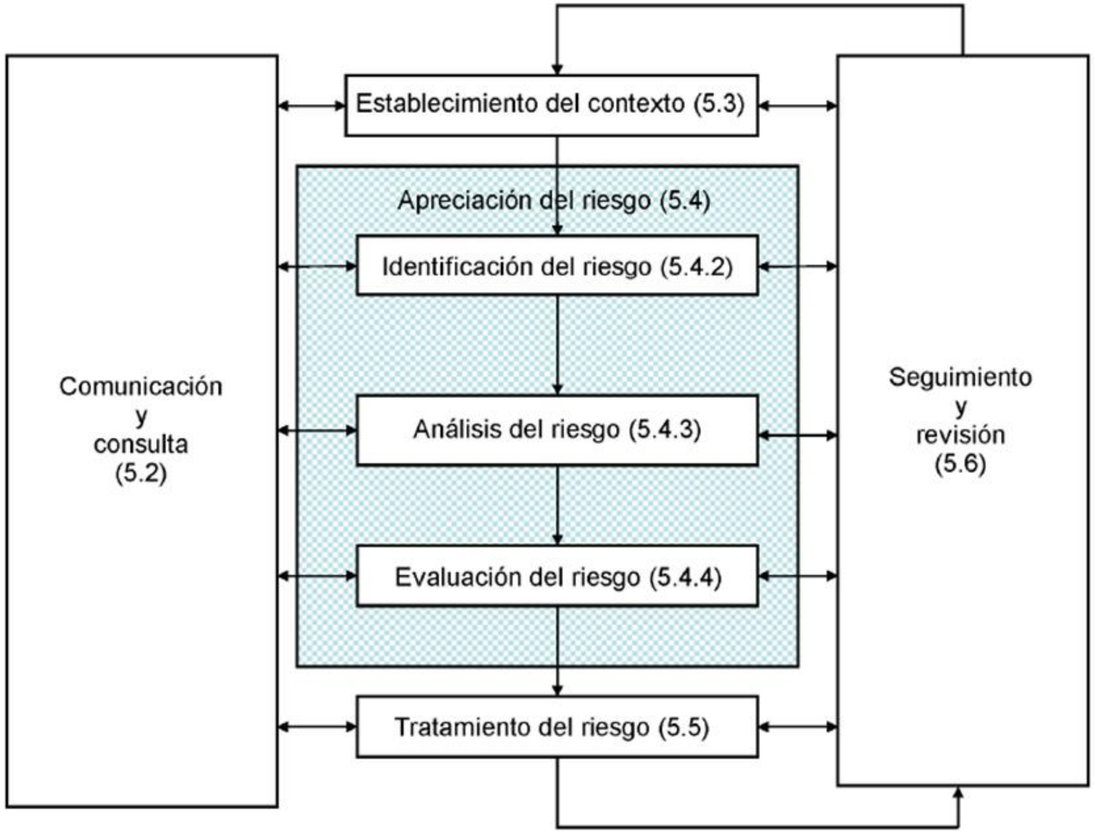
Desde la Dirección, hasta el trabajador con la tarea menos crítica.

Análisis de riesgos

Proceso de gestión de riesgos

Los tres puntos centrales (Identificación del riesgo, Análisis del riesgo y Evaluación del riesgo) corresponden al propio ejercicio de **análisis de riesgos**.

Los otros cuatro procesos restantes que los rodean (Comunicación y Consulta, Establecimiento del Contexto, Tratamiento del riesgo y Seguimiento y Revisión) son propios de la gestión de riesgo a nivel de empresa.



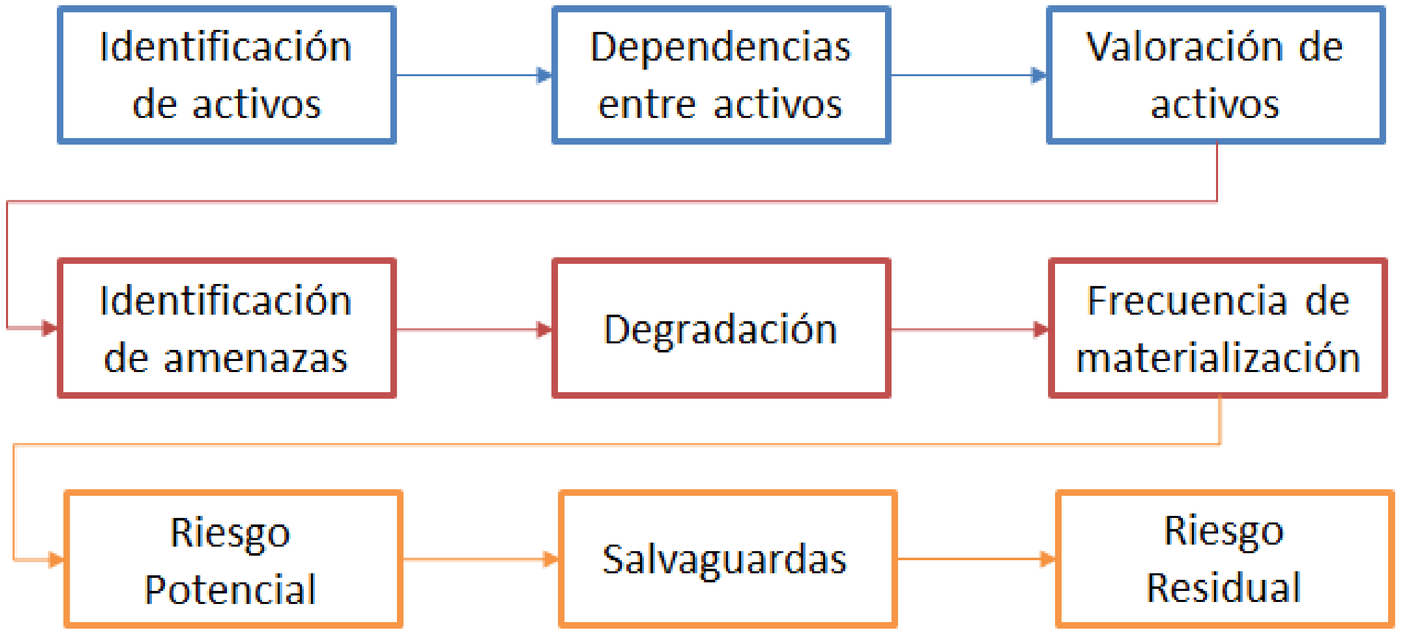
Análisis de riesgos

Proceso de gestión de riesgos

Establecimiento del Contexto:	• Este proceso sirve para definir el nivel al que se quiere realizar el análisis de riesgos. Adicionalmente, se deben establecer los criterios que marcan la gestión de riesgos, como el "apetito de riesgo" o los umbrales que determinan las valoraciones de los catálogos.
Comunicación y Consulta:	• En este proceso se realiza el flujo de información entre los equipos involucrados en el análisis de los riesgos y los distintos interesados que pueden verse afectados por los riesgos y/o por los controles correspondientes. La comunicación da información a los interesados y la consulta obtiene sus reacciones que deben tenerse en cuenta en la toma de decisiones.
Seguimiento y Revisión:	• El objetivo de este proceso es asegurar el cumplimiento de los objetivos de los procesos de Gestión del Riesgo. Se monitorizan de forma constante los resultados y se revisan periódicamente los métodos utilizados para conseguir dichos objetivos.
Identificación del riesgo:	• Este proceso debe determinar cuáles son los eventos de riesgo relevantes para la organización. El catálogo de eventos de riesgos tecnológicos se realiza en base a los eventos de riesgo definidos en los distintos estándares, normas legislativas y sobre todo la experiencia. Según vaya adquiriendo madurez, nuestro sistema de riesgos irá aumentando y mejorando su catálogo de riesgos.
Análisis del riesgo:	• Este proceso determina los niveles de riesgo de cada uno de los eventos identificados anteriormente en base a los parámetros definidos en el modelo de análisis de riesgos.
Valoración de riesgos:	• El objetivo de este proceso es la consolidación de todos los elementos de riesgo analizados en el "Mapa de riesgo tecnológico". La centralización de los riesgos de todos los procesos en un repositorio único permite que las áreas involucradas determinen la valoración del nivel de riesgo de forma holística.
Tratamiento de riesgos:	• Este proceso es el encargado de determinar las acciones de respuesta a los riesgos identificados en el proceso anterior. A que se desarrolla el plan de tratamiento de riesgos.

Análisis de riesgos

El proceso de gestión de riesgos



Análisis de riesgos

Identificación de activos

Primero tendremos que conocer que es un activo:

> "*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, equipos, comunicaciones, recursos administrativos, físicos y humanos…**[UNE 71504:2008]***"

Como hemos expuesto anteriormente existen varios tipos de activos, para organizar, clasificar y valorar adecuadamente un sistema, una aplicación, un proceso e incluso un organización completa se ha decidido crear dos categorías de activos esenciales: **La información y los Servicios.**

Subordinados y dependientes se identifican el resto de activos

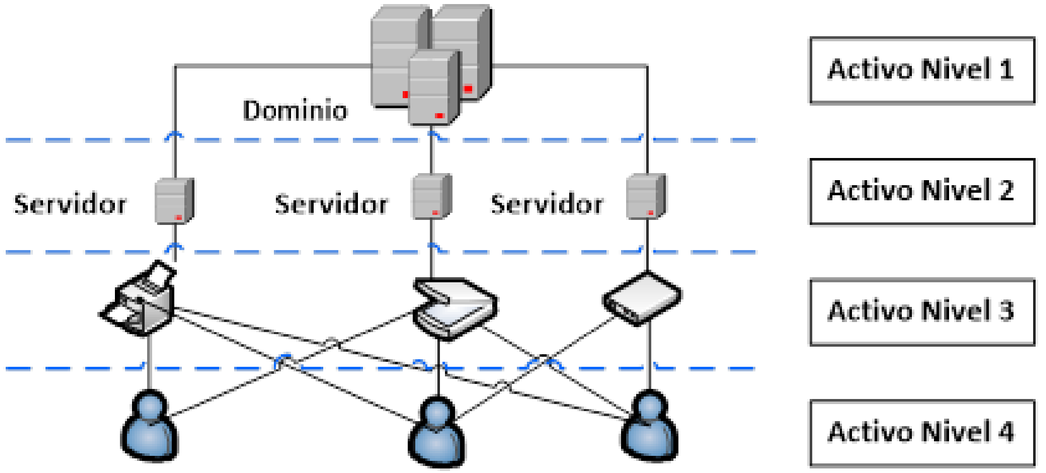
Datos, que materializan la información.
Servicios auxiliares, que se necesitan para poder organizar el sistema.
Las aplicaciones informáticas (software), que permiten manejar los datos.
Los equipos informáticos (hardware), y que permiten hospedar datos, aplicaciones y servicios.
Los soportes de información, 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

Análisis de riesgos

Dependencias

Los activos vienen a formar árboles o grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en la estructura o niveles superiores depende de los activos que se encuentran más abajo o en niveles inferiores. Estas estructuras reflejan de arriba hacia abajo las dependencias, mientas que de abajo hacia arriba la propagación del daño caso de materializarse las amenazas.

Estos activos pueden ser los equipos, las comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos.



Análisis de riesgos

Valoración de activo

Su confidencialidad:	¿Qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
Su integridad:	¿Qué daño causaría que estuviera corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
Su disponibilidad:	¿Qué daño causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.
Su privacidad:	¿Qué daño causaría si afectase a datos de carácter personal?. Esta valoración es típica tanto de datos como de servicios.

Análisis de riesgos

Identificación de amenazas

¿Qué es una amenaza?

Las amenazas son “situaciones que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede afectar a los activos y degradarlos.

“Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008]”.

Al igual que con los activos existen distintos tipos de amenazas:

De origen natural	• Terremotos, inundaciones, etc. Ante estas situaciones el sistema puede ser víctima pasiva, pero se debe tener en cuenta lo que puede suceder.
Del entorno (de origen industrial)	• Contaminación, fallos eléctricos, etc. Ante los cuales el sistema también puede ser víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.
Defectos de las aplicaciones	• Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, ‘vulnerabilidades.
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.
Causadas por las personas de forma deliberada	• Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

Análisis de riesgos

Valoración de amenazas

Una vez que se ha decidido a que activo/s y dimensión/es afecta la amenaza se debe valorar el modo en el que afecta, para ello se debe tener en cuenta el nivel de degradación y la probabilidad.

Nivel de degradación:	Probabilidad:
• Indicaría el nivel de afectación que sufriría el valor del activo, si llegase a materializarse la amenaza.	• Grado de incertidumbre de que se materialice la amenaza.

Análisis de riesgos

Riesgo potencial

¿Qué es el riesgo?

Es la 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. [UNE-ISO Guía 73:2010] Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización. [Magerit:1997]

RIESGO POTENCIAL =
IMPACTO X PROBABILIDAD

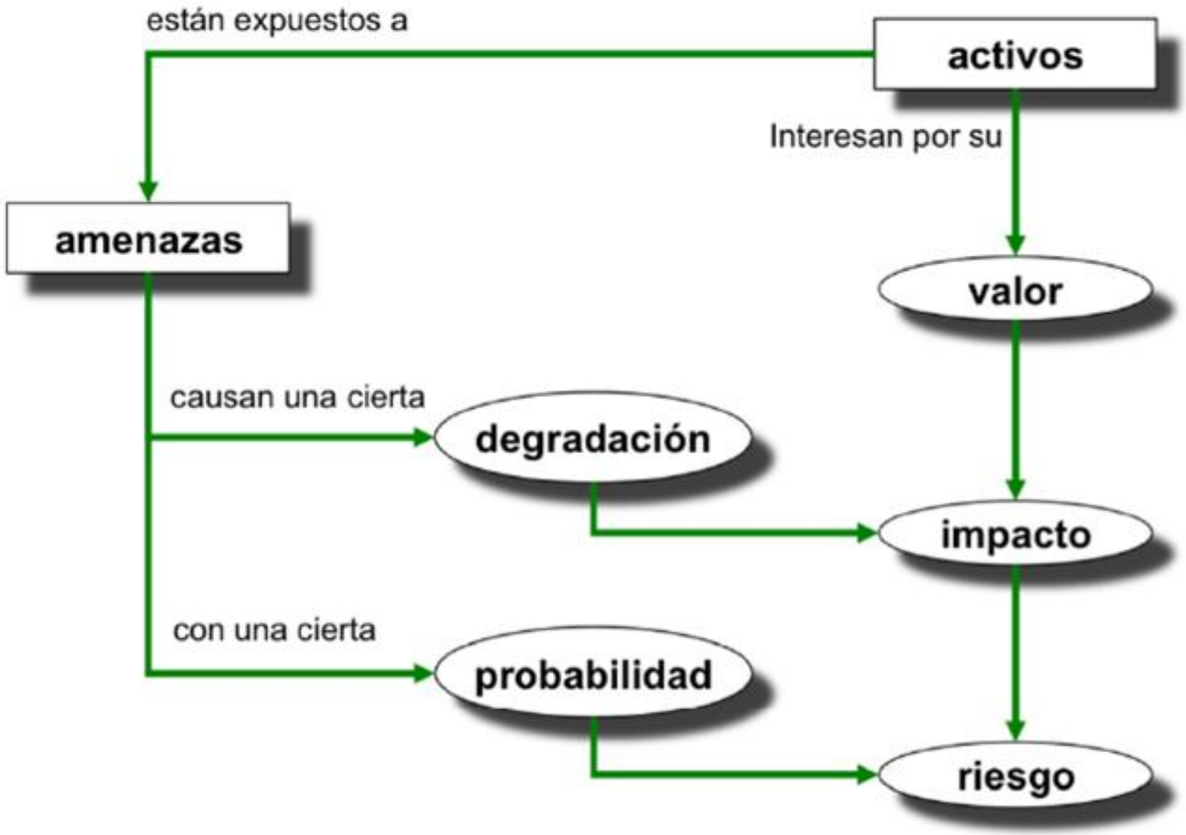
SIN MEDIDAS DE SEGURIDAD

Riesgo Potencial: el riesgo si no hubiera medidas de seguridad. Es el riesgo intrínseco de cada actividad, sin tener en cuenta medidas de seguridad.

Impacto	Es el daño que sufre un activo derivado de la materialización de una amenaza. Por lo tanto conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo calcular el impacto.
Probabilidad	La probabilidad o frecuencia de materialización de un incidente, es la posibilidad de que se materialice una amenaza.

Análisis de riesgos

Riesgo potencial

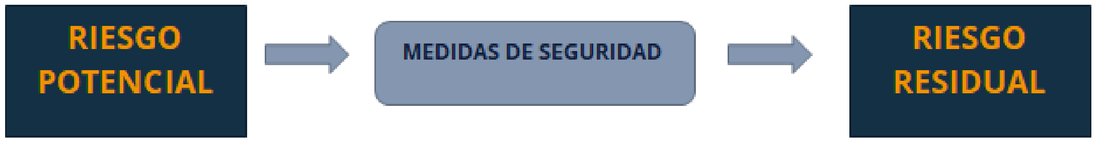


Análisis de riesgos

Medidas de seguridad (Salvaguardas)

El análisis de riesgos ha indicado cuáles son los activos con más riesgos, se ha identificado también cuáles son las principales amenazas que atentan contra estos activos. El siguiente paso es proponer un conjunto de medidas de seguridad, contra medidas, salvaguardas o controles para mitigar los riesgos.

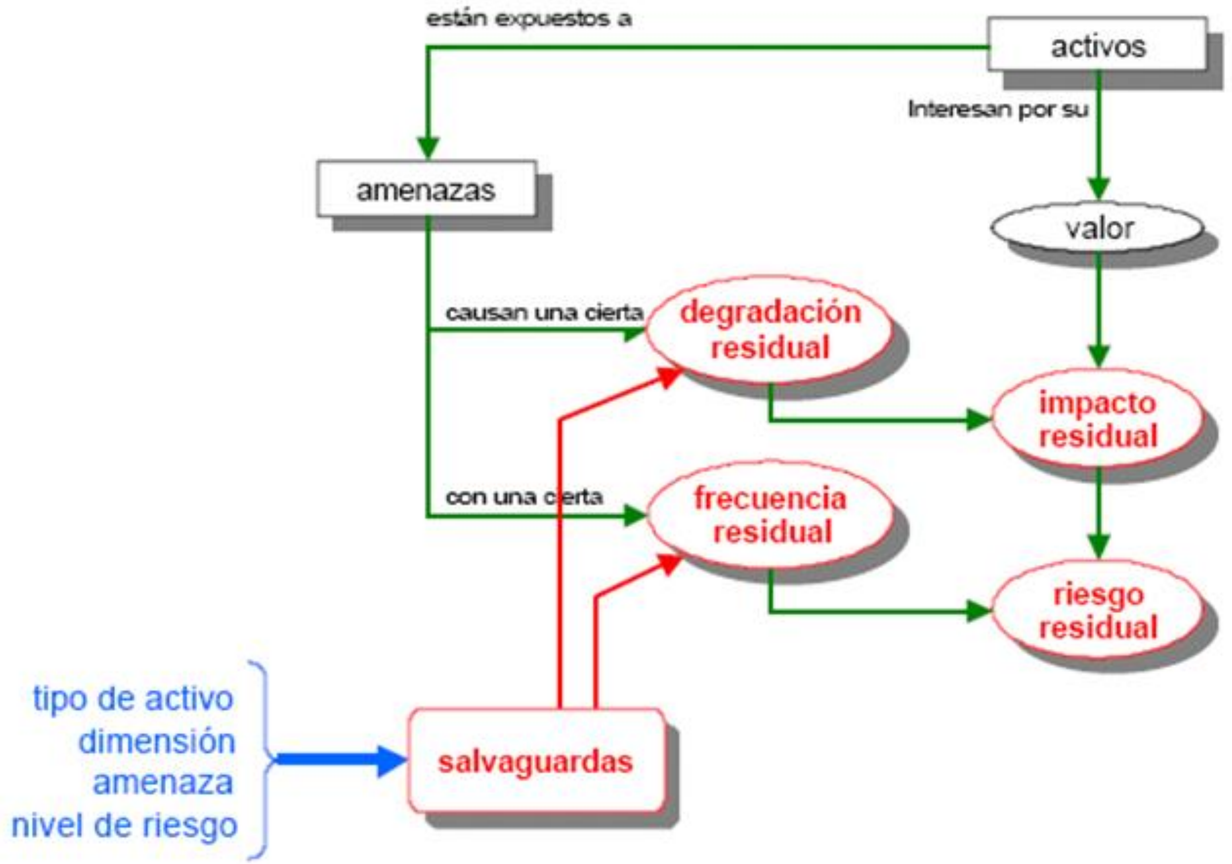
Definimos las medidas de seguridad como aquellos procedimientos o mecanismos tecnológicos (o no) que reducen el riesgo. Hay amenazas que se conjuran simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otras seguridad física y, por último, está la política de personal.

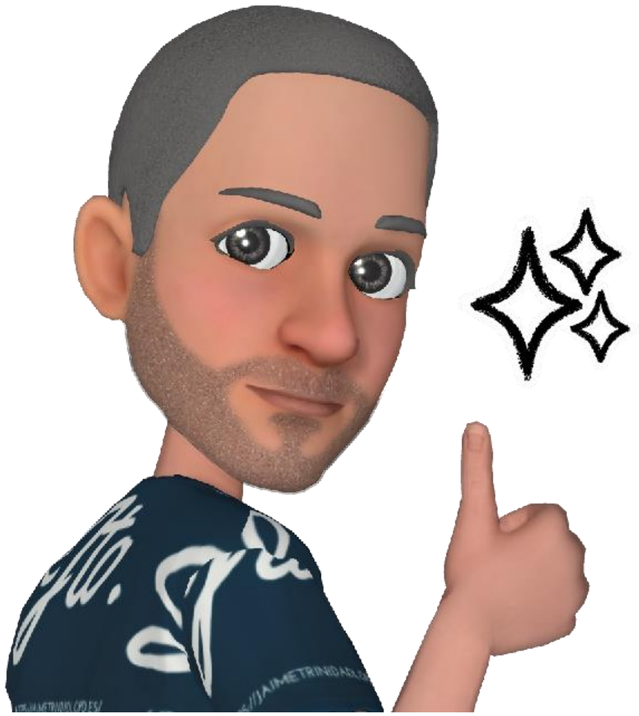


Análisis de riesgos

Riesgos residual

Es aquel riesgo que subsiste, después de haber implementado controles. Es importante advertir que el nivel de riesgo al que está sometido una compañía nunca puede erradicarse totalmente. Por ello, se debe buscar un equilibrio entre el nivel de recursos y mecanismos que es preciso dedicar para minimizar o mitigar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable).





EL PRÓXIMA DÍA, MEDIDAS DE CONTENCIÓN Y MITIGACIÓN

https://jaimetrinidadlopd.es/

Jaime T. Ortiz

CONSULTOR DE SEGURIDAD DE LA INFORMACION

HTTPS://JAIMETRINIDADLOPD.ES/

sedian Seguridad Digital de Andalucía