CURSO DE SEGURIDAD INFORMATICA

7.1. MF0486_3 SEGURIDAD EN EQUIPOS INFORMATICOS

TEMA 1 : Criterios generales comúnmente aceptados sobre seguridad de los equipos informáticos (5 horas)

- Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
- Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
- Salvaguardas y tecnologías de seguridad más habituales
- La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Activos de información

Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones **funcionen y consigan los objetivos** que se han propuesto por la alta dirección.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Inventario de activos de información

Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos de información importantes de la organización.

Todos los activos de información deben ser propiedad de una parte designada de la organización. En este sentido, el propietario del activo definirá y garantizará los controles para la adecuada protección del activo. Adicionalmente, los activos de información en este inventario deben clasificarse en términos de confidencialidad, integridad y disponibilidad.

Para realizar este inventario se recomienda hacer una clasificación. Una clasificación recomendada por expertos es la siguiente.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Inventario de activos de información pura

Datos digitales

- Personales
- Financieros
- Legales
- Investigación y desarrollo
- Estratégicos
- Comerciales
- Correo electrónico
- Contestadores automáticos
- Bases de datos
- Unidades lógicas
- Copias de seguridad

Activos tangibles

- Personales
- Financieros
- Legales
- Investigación y desarrollo
- Estratégicos y comerciales
- Correo electrónico
- Otro materiales de copia de seguridad
- Llaves de oficinas
- Otros medios de almacenamiento

Activos intangibles

- Conocimiento
- Relaciones
- Secretos comerciales
- Licencias
- Patentes
- Experiencia
- Conocimientos técnicos
- Imagen corporativa
- Marca
- Reputación comercial
- Confianza de los clientes
- Ventaja competitiva
- Ética
- Productividad

Software de aplicación

- Propietario desarrollo por la organización
- Cliente
- Planificación de recursos empresariales
- Gestión de la información
- Utilidades
- Herramientas de bases de datos
- Aplicaciones de comercio electrónico
- Middleware

Sistemas operativos

- Servidores
- Ordenadores de sobremesa
- Ordenadores contrales
- Dispositivos de red
- Dispositivos de mano e incrustados

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Inventario de activos físicos

Infraestructura de TI

- Edificios
- Centros de datos
- Habitaciones de equipos y servidores
- Armarios de red
- Oficinas
- Escritorios
- Cajones
- Archivadores
- Salas de almacenamiento de medios físicos
- Cajas de seguridad
- Dispositivos de identificación
- Autentificación
- Control de acceso al personal
- Otros dispositivos de seguridad

Activos de servicios de TI

- Servicios de autenticación de usuario
- Administración de procesos
- Enlaces
- Cortafuegos
- Servidores proxy
- Servicios de red
- Servicios inalámbricos
- Anti-spam
- Virus
- Spyware
- Detección y prevención de intrusiones
- Teletrabajo
- Seguridad
- Correo electrónico
- Mensajería instantánea
- Servicios web
- Contratos de soporte
- Mantenimiento de software

Controles de entorno de TI

- Equipos de alarma
- Supresión contra incendio
- Sistemas de alimentación ininterrumpida
- Alimentación de potencia
- Acondicionadores
- Filtros
- Supresores de potencia
- Deshumificadores
- Refrigeradores
- Alarmas de aire
- Alarmas de agua

Hardware de TI

- Dispositivos de almacenamiento
- Ordenadores de mesa
- Estaciones de trabajo
- Ordenadores portátiles
- Equipos de mano
- Servidores
- Módems
- Líneas de terminación de red
- Dispositivos de comunicaciones
- Equipos multifunción

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Inventario de activos humanos

Empleados

- Personal y directivos
- Participar los que tienen roles de gestión como altos cargos
- Arquitectos de software y desarrolladores
- Administradores de sistemas
- Administradores de seguridad
- Operadores
- Abogados
- Auditores
- Usuarios con poder
- Expertos en general

Externos

- Trabajadores temporales
- Consultores externos
- Asesores especialistas
- Contratistas especializados
- Proveedores
- Socios

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

La información es el **activo** más importante de su organización, por ello entendemos la importancia de contar con un sistema sólido para administrarla y protegerla

SEGURIDAD DE LA INFORMACIÓN

Para la norma ISO 17799 e ISO 27001,la seguridad de la información es “la preservación de confidencialidad, integridad y disponibilidad de la información”.

Se trata pues, de proteger la información en varias facetas o propiedades.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

¿Cómo funciona la ISO 27001?

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Triada de la Seguridad" o "CIA"

- **La confidencialidad** (Confidentiality), es decir, que la información solo esté accesible para quien esté autorizado a ello.
- **La integridad** (Integrity), es decir, que la información sea exacta y completa, de manera que solo pueda modificarla quien esté autorizado a ello.
- **La disponibilidad** (Availability), es decir, que la información esté accesible cuando sea necesario.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

La información es el **activo** más importante de su organización, por ello entendemos la importancia de contar con un sistema sólido para administrarla y protegerla

SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información pretende que los sistemas y equipos de información sean fiables, es decir, que su comportamiento sea predecible, acorde con su diseño y construcción. La fiabilidad o seguridad, de acuerdo con la definición de la norma ISO 17799, mencionada en el epígrafe anterior, se apoya en tres aspectos o "principios de seguridad" esenciales: **La triada CIA**

Es imposible alcanzar la completa ausencia de inseguridad, o lo que es lo mismo, no existe la seguridad total.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Amenazas, vulnerabilidades e incidentes de seguridad

Las amenazas son las posibles acciones que dañarían los equipos informáticos. Para causar el daño, la amenaza debe encontrar un punto en que afecte al equipo; este punto es una vulnerabilidad del equipo ante la amenaza.

La vulnerabilidad, por lo tanto, permite o facilita que una amenaza dañe el equipo; mientras que la amenaza es cualquier hecho que, intencionadamente o no, aprovecha una vulnerabilidad para dañar un equipo.

Un Incidente de seguridad, pasa cuando una amenaza o un conjunto de ellas sucede, y aprovecha una vulnerabilidad, cuyo efecto es un daño o impacto al equipo informático.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

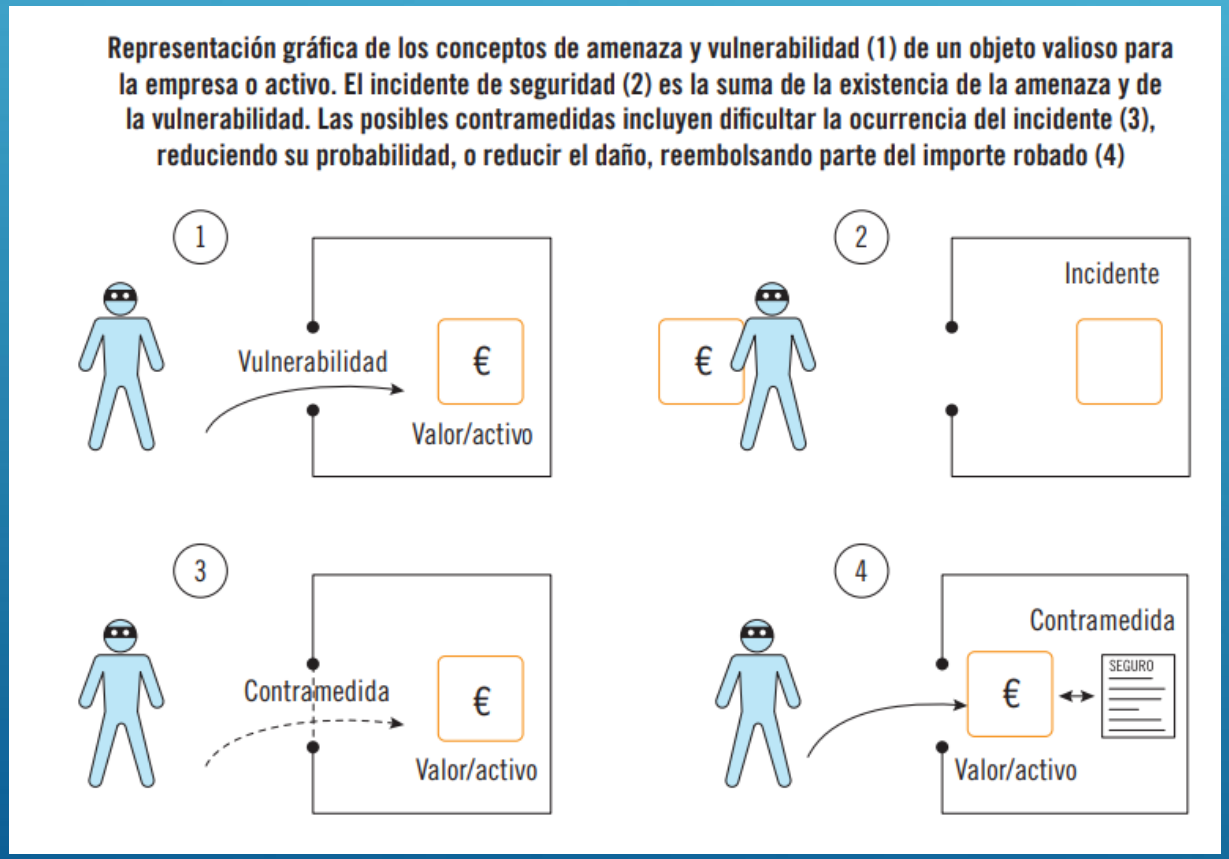
Amenazas, vulnerabilidades e incidentes de seguridad

Normalmente, las amenazas serán genéricas, y no se podrán eliminar por completo, mientras que las vulnerabilidades serán particulares de cada equipo, y sí permiten intervenir en ellas.

Frente a los incidentes de seguridad, se deben disponer contramedidas o salvaguardas que fortalezcan el sistema. Las contramedidas persiguen conocer, prevenir, impedir, reducir y controlar el daño que podría tener un equipo.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

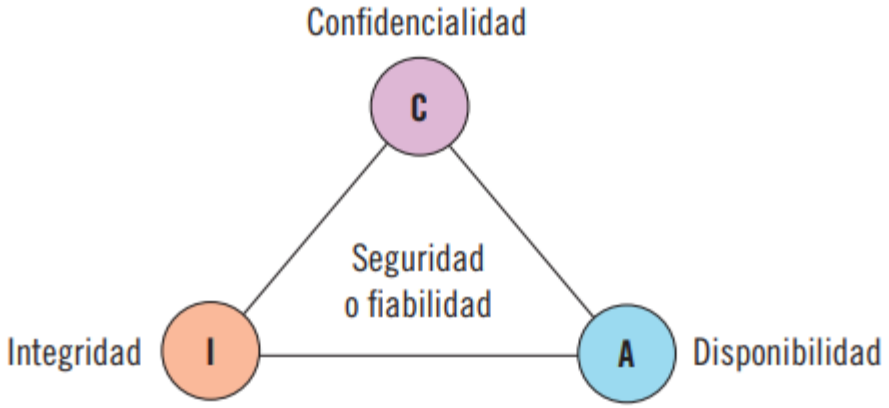
Amenazas, vulnerabilidades e incidentes de seguridad



1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Amenazas, vulnerabilidades e incidentes de seguridad

Representación gráfica de los principios de seguridad de la información.La información es segura o fiable cuando hay confidencialidad, integridad y disponibilidad



1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Amenazas, vulnerabilidades e incidentes de seguridad

Por ejemplo, si la amenaza de un virus informático capaz de capturar el tráfico de red y reenviarlo, aprovecha la vulnerabilidad del sistema de correo electrónico de enviar las contraseñas sin cifrar, el atacante obtendría la contraseña del correo, y podría leerlo, viéndose comprometida la confidencialidad del correo electrónico.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Amenazas, vulnerabilidades e incidentes de seguridad

Por ejemplo, si la amenaza del extravío de una tarjeta magnética de identificación, aprovecha la vulnerabilidad de que el sistema de autenticación de usuarios solo necesite de dicha tarjeta, quien la encuentre podría modificar la información de una base de datos, como si fuera el usuario autorizado, viéndose comprometida la integridad de la información.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Amenazas, vulnerabilidades e incidentes de seguridad

Por ejemplo, si la amenaza de un corte de suministro eléctrico aprovecha la vulnerabilidad de que el equipo informático no dispone de un sistema de alimentación ininterrumpida, el equipo no se podría encender, viéndose comprometida la disponibilidad de la información cuando se necesite.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Riesgo de un incidente de seguridad

El riesgo es una medida del daño probable que causará una amenaza, que aprovecha una vulnerabilidad para causar un daño. Es mayor cuanto más frecuente sea la aparición de la amenaza, y cuanto mayor sea el daño del incidente que acarree. Una aproximación cuantitativa sencilla es emplear la siguiente fórmula:

Riesgo = (probabilidad de ocurrencia de la amenaza) x (impacto o daño)

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Riesgo de un incidente de seguridad

Se puede reducir el riesgo, añadiendo las contramedidas que reduzcan las vulnerabilidades a las posibles amenazas. Cuantas más contramedidas se dispongan, es decir, cuantos más recursos se dediquen a la seguridad de los equipos informáticos, menor es el daño probable, o lo que es lo mismo, menor es el riesgo para el sistema de información.

Existirá un balance entre el riesgo de un incidente de seguridad y los recursos que se dediquen a reducir su daño probable.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

:

Riesgo de un incidente de seguridad

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

¿Dónde interviene la gestión de seguridad de la información en una empresa?

Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información:

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Riesgo de un incidente de seguridad (Modelo de seguridad)

Este balance debe ser gestionado de una manera metódica por varias razones, pero principalmente por las siguientes:

- Para poder analizar la viabilidad de la inversión en seguridad. Es necesario justificar la inversión de recursos en seguridad, y para ello, hay que poder determinar mediante un método los riesgos existentes, antes y después de la inversión.

- Para poder analizar la mejora o no, en el cumplimiento de los objetivos de la seguridad de la información a lo largo del tiempo. Es necesario poder evaluar de una manera sistemática el estado de riesgo de los sistemas de información de una empresa, por ejemplo, en auditorías internas anuales, o quizá mediante auditorías externas, a las que esté obligada la empresa por alguna ley.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Riesgo de un incidente de seguridad
(Modelo de seguridad)

Este método sistemático, que se precisa para decidir cuánto riesgo asume la empresa, constituye lo que se denomina un "modelo de seguridad".

El modelo de seguridad persigue organizar los procesos de gestión de la seguridad de la información, en base a unas directrices (que pueden ser estrategias empresariales, normativas cuyo cumplimiento se quiera certificar para poder exportar los productos o prestar los servicios o, sencillamente, leyes que se esté obligado a cumplir), y algún método para calcular los riesgos del sistema de información.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Riesgo de un incidente de seguridad (Modelo de seguridad)

Para estudiar el riesgo, existen dos pasos claramente diferenciados:

- **El análisis de riesgos,** que consiste en identificar amenazas, determinar las vulnerabilidades, y medir el impacto o daño que causaría un incidente. Se pueden emplear métodos cuantitativos (como en la aplicación práctica anterior), o cualitativos (valorando el riesgo en muy alto, alto, bajo, medio, etc.), para ordenar los riesgos.

- **La gestión de riesgos**, que partiendo de los resultados del análisis de riesgos, y una vez determinados los criterios para aceptar un riesgo (legales, económicos, etc.), permite elegir las contramedidas de seguridad que se implantarán.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Riesgo de un incidente de seguridad
(Modelo de seguridad)

El análisis y gestión de riesgos aporta un valor extraordinario a la gestión de seguridad, reduciendo la probabilidad de fracaso de una empresa, y protegiéndola, al ser una herramienta que facilita que la actividad futura se realice de manera efectiva y controlada.

Resumidamente, un Modelo de Seguridad orientado a la gestión del riesgo, emplea el cálculo del riesgo, y unos criterios empresariales (normativa, legislación, etc.), para poder decidir si es viable reducir el riesgo que se asume, o no.

NOTA : Hacer Ejemplo Página 16

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Tratamiento de riesgos
(Modelo de seguridad)

En este punto estamos preparados para definir la política de tratamiento de los riesgos en función de la probabilidad de que las amenazas o las vulnerabilidades propias del activo puedan causar un daño total o parcial al activo de la información.

Esta definición debe alinearse con la disponibilidad, confidencialidad e integridad del mismo y con la política definida por la dirección.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Tratamiento de riesgos

En este punto, se seleccionan las acciones adecuadas para cada riesgo, las cuales irán orientados a:

- **Asumir el riesgo:** se trata de no hacer nada. Simplemente, sabemos que no tenemos cómo evitarlo y debemos convivir con él. Las organizaciones deciden aceptar un riesgo cuando la probabilidad de que ocurra esmuy baja.

- **Reducir el riesgo:** Se usa cuando eliminar completamente el riesgo resulta mucho más costoso que asumir las consecuencias negativas de que este llegara a materializarse.

- **Eliminar el riesgo:** Se implementan las acciones para hacer que las condiciones o los factores que pueden generar el riesgo desaparezcan y con ellos el riesgo. Esta es una opción para aquellos casos de alta probabilidad de ocurrencia, con un muy alto impacto negativo.

- **Transferir el riesgo:** Significa que pasamos el problema a alguien más. La forma más usual de transferir un riesgo es contratar una póliza de seguros que indemnice a la organización en caso de que se presente el problema.

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Tratamiento de riesgos

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Tratamiento de riesgos
(Mapa de calor)

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

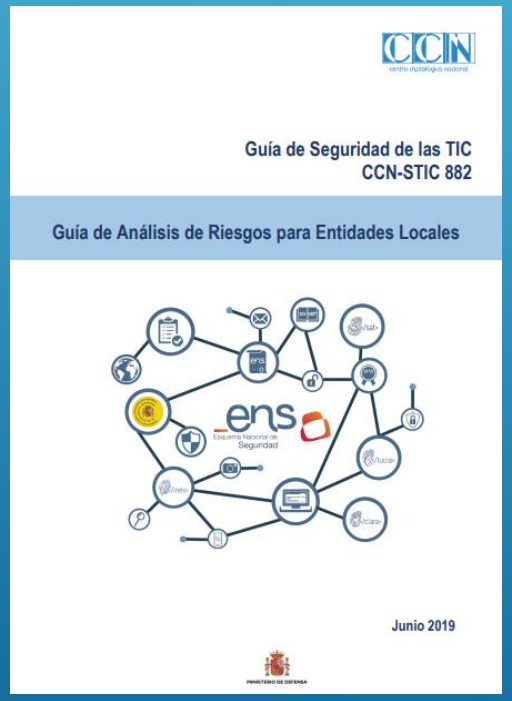
Tratamiento de riesgos
(Mapa de calor)

El anterior ejemplo muestra un mapa de riesgos en el que se tienen:

1. Daño por tormentas (riesgo operacional).
2. Ciberataque y robo de información (riesgo operacional).
3. Comentario negativo en redes sociales (riesgo reputacional).
4. Número significativo de clientes cambiándose a la competencia (riesgo estratégico).

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Gestión de riesgos
(Guias)

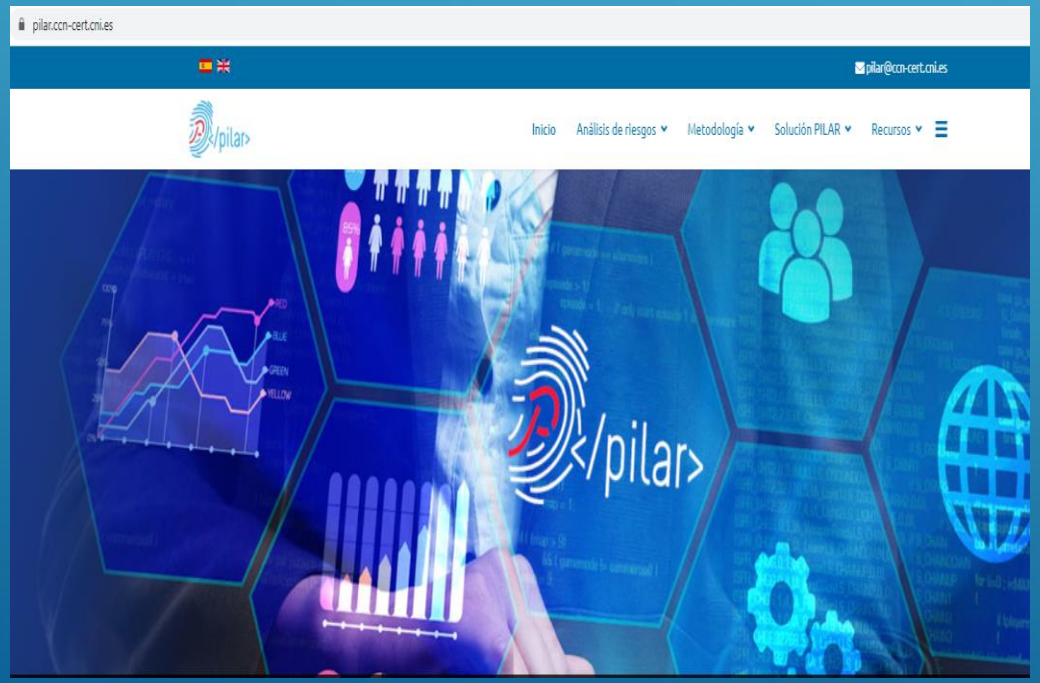


CURSO DE SEGURIDAD INFORMATICA

1.1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

Gestión de riesgos

(Software : Pilar)



1.2. Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes

Las amenazas a las que está expuesto un sistema de información son muy diversas, por lo que, al menos en la fase inicial de la gestión de riesgos, conviene centrarse en las principales.

Posteriormente, se podrá mejorar el modelo, aumentando el catálogo de amenazas. Para esa selección inicial, ayudará un amplio y polifacético conocimiento de la empresa: su organigrama, sus procesos productivos, su localización geográfica, su competencia, etc. Por ejemplo, si una empresa tiene dos sucursales, una en una zona de interior, y otra muy próxima al mar, para esta segunda sucursal, puede ser importante analizar el riesgo de exposición a un alto nivel de humedad relativa del aire.

1.2. Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes

Para determinar las amenazas, o encontrar nuevas, ayudará saber que pueden clasificarse como:

- Amenazas naturales o artificiales.
- Amenazas debidas al entorno (ambiente), o debidas al hombre.
- Amenazas accidentales o intencionadas.

A continuación, se expone un conjunto de amenazas frecuentes, extraído del catálogo de amenazas de MAGERIT (e-Admin) , que no pretende ser exhaustivo, aunque probablemente cubrirá la mayoría de situaciones generales, así como algunos de los riesgos principales, y salvaguardas usuales.

NOTA : Ver página 19

1.3. Salvaguardas y tecnologías de seguridad más habituales

Las salvaguardas, o contramedidas, persiguen detectar, prevenir, impedir, reducir, y controlar una amenaza y el daño que pueda generar. Son elementos de defensa, para que las amenazas no causen tanto daño. Como en el caso de las amenazas, las salvaguardas se pueden clasificar según distintas categorías. Por ejemplo, existirán:

- Salvaguardas preventivas o proactivas, que persiguen anticiparse a la ocurrencia del incidente.

- Salvaguardas reactivas, que persiguen reducir el daño una vez ocurre el incidente.

- Salvaguarda de "no hacer nada", o de aceptar el riesgo existente para los equipos (cuando se cumplan los criterios de aceptación de riesgo de la empresa, y solo cuando esta decisión sea autorizada por la Dirección).

1.3. Salvaguardas y tecnologías de seguridad más habituales

Las salvaguardas, o contramedidas, persiguen detectar, prevenir, impedir, reducir, y controlar una amenaza y el daño que pueda generar. Son elementos de defensa, para que las amenazas no causen tanto daño. Como en el caso de las amenazas, las salvaguardas se pueden clasificar según distintas categorías. Por ejemplo, existirán:

- Salvaguardas preventivas o proactivas, que persiguen anticiparse a la ocurrencia del incidente.

Por ejemplo, son salvaguardas preventivas las relacionadas con los controles de acceso de los usuarios a los equipos, como el uso de contraseñas. Controlando el acceso de los usuarios exclusivamente a la información que necesitan conocer para el desempeño de su trabajo, se previenen daños a la confidencialidad e integridad de la información.

1.3. Salvaguardas y tecnologías de seguridad más habituales

Las salvaguardas, o contramedidas, persiguen detectar, prevenir, impedir, reducir, y controlar una amenaza y el daño que pueda generar. Son elementos de defensa, para que las amenazas no causen tanto daño. Como en el caso de las amenazas, las salvaguardas se pueden clasificar según distintas categorías. Por ejemplo, existirán:

- Salvaguardas reactivas, que persiguen reducir el daño una vez ocurre el incidente.

Por ejemplo, son salvaguardas de carácter reactivo las copias de seguridad. Las copias no evitan que se produzca un incidente que derive en pérdida de información, pero sí reducen el daño limitando la pérdida a la información modificada desde la última copia de seguridad verificada.

1.3. Salvaguardas y tecnologías de seguridad más habituales

Las salvaguardas, o contramedidas, persiguen detectar, prevenir, impedir, reducir, y controlar una amenaza y el daño que pueda generar. Son elementos de defensa, para que las amenazas no causen tanto daño. Como en el caso de las amenazas, las salvaguardas se pueden clasificar según distintas categorías. Por ejemplo, existirán:

- Salvaguarda de "no hacer nada", o de aceptar el riesgo existente para los equipos (cuando se cumplan los criterios de aceptación de riesgo de la empresa, y solo cuando esta decisión sea autorizada por la Dirección).

Como aclaración de salvaguarda de "no hacer nada", se tomará de ejemplo una empresa, cuya política de seguridad establece que se aprobarán los riesgos, cuando sean inferiores al 10 % del valor de los activos. Si el análisis de riesgos establece que este es del 5 % del valor de los equipos, puede decidirse asumirlo, y no interponer salvaguardas para reducirlo; pero siempre debe ponerse en conocimiento de la Dirección, que es el órgano responsable en última instancia del riesgo que se asume.

1.3. Salvaguardas y tecnologías de seguridad más habituales

Las fases de esta metodología son los siguientes:

1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

A la vista de la multitud de amenazas y salvaguardas consideradas, no se puede enfrentar el problema mediante un conjunto de medidas de seguridad aisladas para objetos concretos. Es decir, se pueden interponer multitud de salvaguardas y mecanismos de seguridad, pero estas salvaguardas por sí mismas, no aportan suficientes garantías de continuidad a la empresa. Es necesaria una gestión adecuada de esas medidas, que incluirá los procesos, revisiones, recalificaciones, y adaptaciones para la realidad cambiante de la empresa, su entorno, sus amenazas y sus debilidades.

Para la construcción de un sistema de seguridad, no bastan los conceptos tecnológicos, sino que se necesitan también aspectos de gestión, aspectos legales, aspectos éticos, u otros específicos de la naturaleza y ambiente interno y externo de la empresa.

1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

Sistema de Gestión de Seguridad de la Información (SGSI)

Es en este punto en el que surge el concepto de Sistema de Gestión de Seguridad de la Información (SGSI), como un sistema de gestión usado para establecer y mantener un entorno seguro. Se trata, sencillamente, de analizar la empresa, y fijar sus necesidades de seguridad iniciales, de poner en práctica las medidas de protección para lograr alcanzar estas necesidades, de ser capaz de medir si se han alcanzado o no, y de detectar las mejoras en las medidas de protección para alcanzar las necesidades.

1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

Elementos o fases para la Implementación de un SGSI

El Sistema de Gestión de La Seguridad de la Información que propone la Norma ISO 27001 se puede resumir en las siguientes fases que se detallan en la figura:

Los Objetivos del SGSI son preservar la:

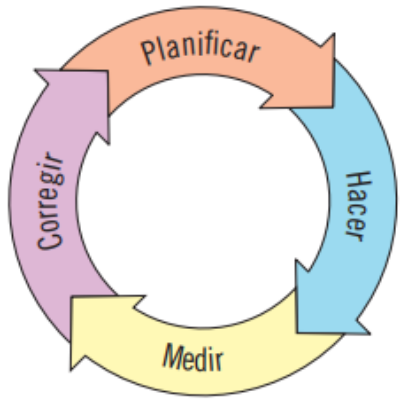
- **Confidencialidad**
- **Integridad**
- **Disponibilidad** de la Información

1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

Sistema de Gestión de Seguridad de la Información (SGSI)

La anterior secuencia describe una repetición continua de fases de planificación (en inglés, plan), ejecución (en inglés, do), medida (en inglés, check) y corrección (en inglés, act), constituyendo un ciclo de mejora continua de Deming (P-D-C-A), como muestra la siguiente imagen.

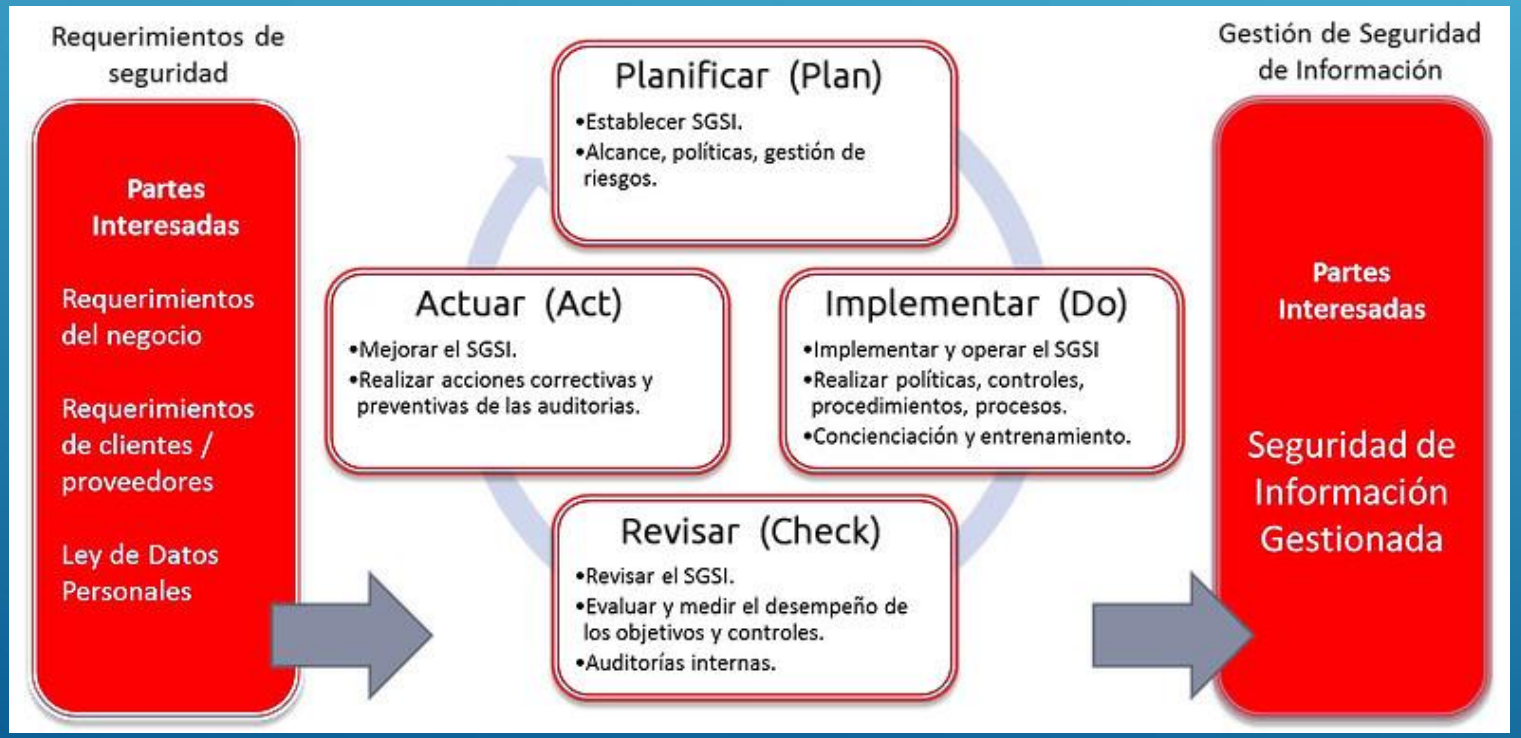
Ciclo de mejora continua de Deming, aplicable al proceso de ejecución de un SGSI



Se analizan o planifican las necesidades de seguridad de la empresa, estableciendo las medidas de protección necesarias para alcanzarlas; se implantan las medidas, se mide el resultado de satisfacción de las necesidades de seguridad, se determinan las correcciones que hay que realizar en las medidas de protección, y se vuelve a comenzar (revisando las necesidades y las medidas que permitirían alcanzar esas necesidades, incluyendo las correcciones detectadas en la ejecución anterior).

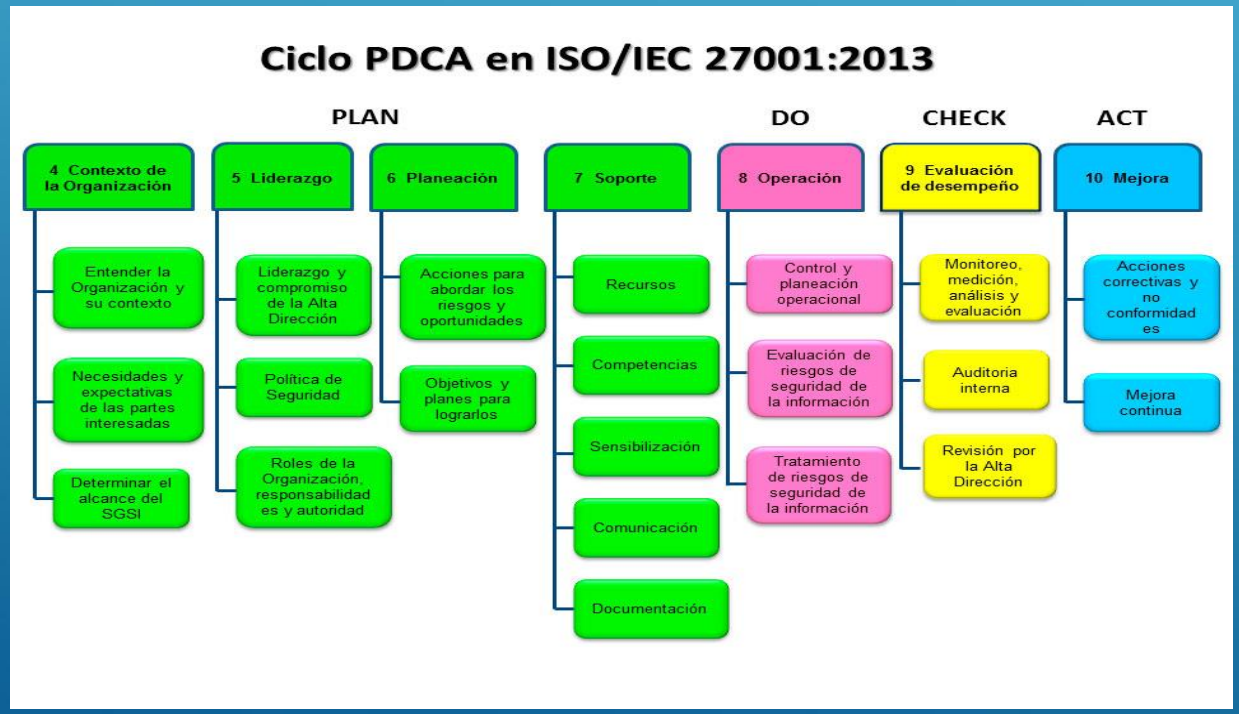
1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

Sistema de Gestión de Seguridad de la Información (SGSI)



1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

Sistema de Gestión de Seguridad de la Información (SGSI)



1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

Sistema de Gestión de Seguridad de la Información (SGSI)

En este proceso de ejecución continuo, no se debe perder de vista el objetivo último que, usando una terminología empresarial, podría enunciarse como “asegurar la continuidad del negocio, minimizando los riesgos, maximizando el retorno de la inversión y permitiendo nuevas oportunidades para la empresa”.

Una empresa pequeña o mediana (PYME) puede enfrentar serias dificultades para abordar la implantación de un SGSI, desde una perspectiva tan compleja y abstracta como la del enunciado anterior. Las normativas y metodologías existentes, algunas ya mencionadas en este capítulo como ISO 17799 y MAGERIT, resultan demasiado amplias y extensas, por su necesaria globalidad para todo tipo de organizaciones.

1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

Sistema de Gestión de Seguridad de la Información (SGSI)

La solución, sin embargo, es nuevamente sencilla, y consiste en aplicar un principio que será muy frecuente en el ámbito de la seguridad de la información: el principio de proporcionalidad, que nos dice que "**las medidas deben adecuarse a sus objetivos**". En el ámbito de la seguridad de la información, "**las salvaguardas deben ser proporcionales al riesgo**".

1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

Sistema de Gestión de Seguridad de la Información (SGSI)

Ejemplo 1 : Para el control de acceso a una estación de trabajo, donde los usuarios realizan labores ofimáticas sobre datos no confidenciales, bastaría inicialmente emplear un sistema de usuario y contraseña, integrado en el propio sistema operativo. Parece una medida proporcional en coste al objetivo de seguridad, que vendrá marcado por el riesgo que introducen en la empresa los sistemas informáticos accesibles desde esos puestos.

Ejemplo 2 : Para el control de acceso a una estación de trabajo, donde los usuarios realizan labores ofimáticas sobre datos no confidenciales, bastaría inicialmente emplear un sistema de usuario y contraseña, integrado en el propio sistema operativo. Parece una medida proporcional en coste al objetivo de seguridad, que vendrá marcado por el riesgo que introducen en la empresa los sistemas informáticos accesibles desde esos puestos.

1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

Sistema de Gestión de Seguridad de la Información (SGSI)

El principio de proporcionalidad permite enfocar adecuadamente un sistema de gestión completo, y se puede afirmar que “el SGSI debe ser proporcional al valor de la continuidad del negocio”.

1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

Sistema de Gestión de Seguridad de la Información (SGSI)

Las herramientas elementales para la correcta gestión de la seguridad informática, no son equipos de alta tecnología y costes inabordables. Las herramientas elementales son dos:

- **La redacción de una política de seguridad de la información**, que recoja de las directrices del SGSI a partir de las cuales derivarán todas las demás acciones. En este libro se empleará el contenido y recomendaciones recogidas en ISO 17799 y en la serie ISO 27000, así como en la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), de manera proporcional a la empresa objetivo de aplicación.

- **La adopción de una metodología sencilla**, que permita evaluar el riesgo. En este libro se empleará el contenido y recomendaciones recogidas en MAGERIT, de manera proporcional a la empresa objetivo de aplicación.

(Otras metodologías)

1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

La serie ISO 27000

La serie ISO 27000 está formada por muchas normas, entre las que destacan:

- ISO 27000: términos y definiciones.
- ISO 27001: requisitos de un SGSI.
- ISO 27002: controles o salvaguardas (muy similar a la ISO 17799).
- ISO 27004: cómo medir la eficacia de un SGSI.
- ISO 27005: gestión de riesgos.
- ISO 27007: auditoria de un SGSI.
- ISO 27011: seguridad de la información para telecomunicaciones

1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

ISO 27001: Cómo hacer tu política del SGSI

1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

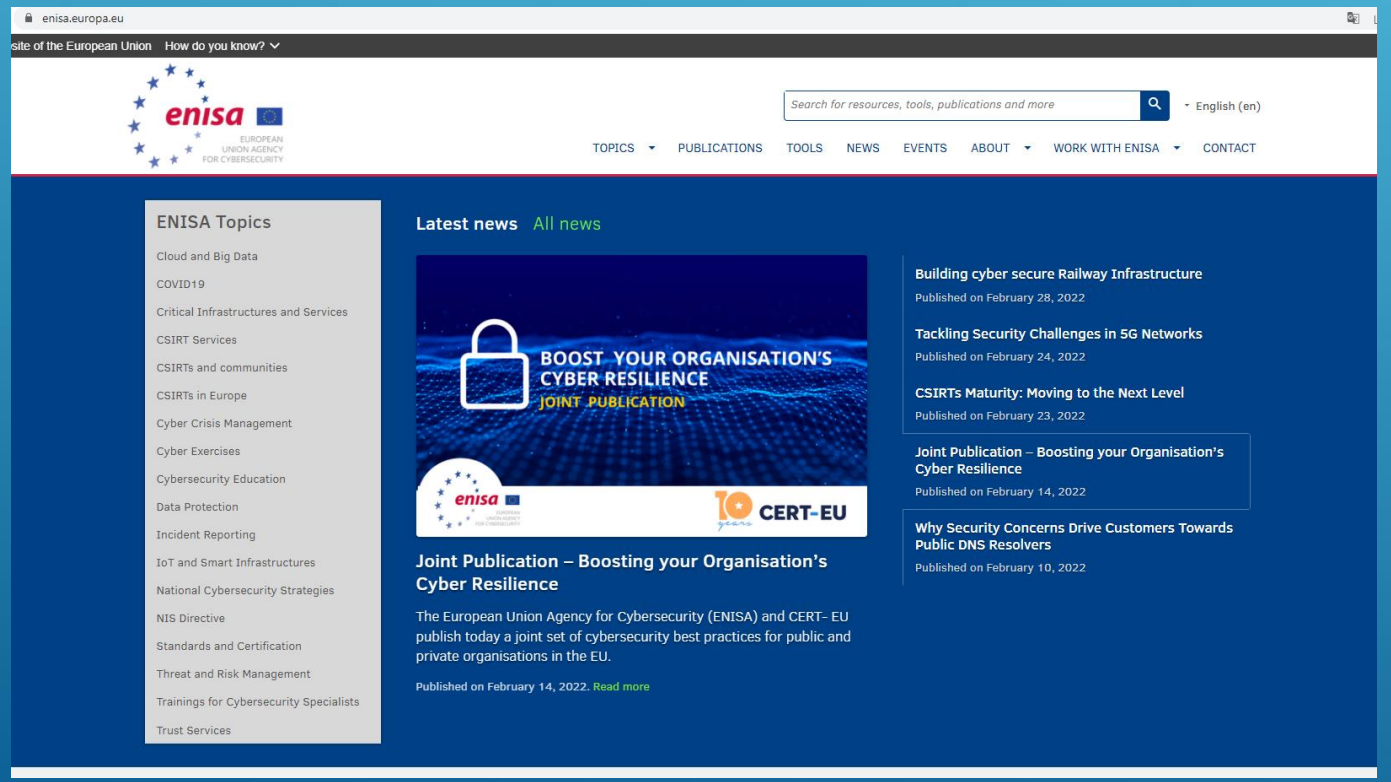
Cyberseguridad

La **seguridad informática**, también conocida como **ciberseguridad**, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras

La definición de seguridad de la información no debe ser confundida con la de «seguridad informática», ya que esta última solamente se encarga de la seguridad en el medio informático, pero por cierto, la información puede encontrarse en diferentes medios o formas, y no exclusivamente en medios informáticos.

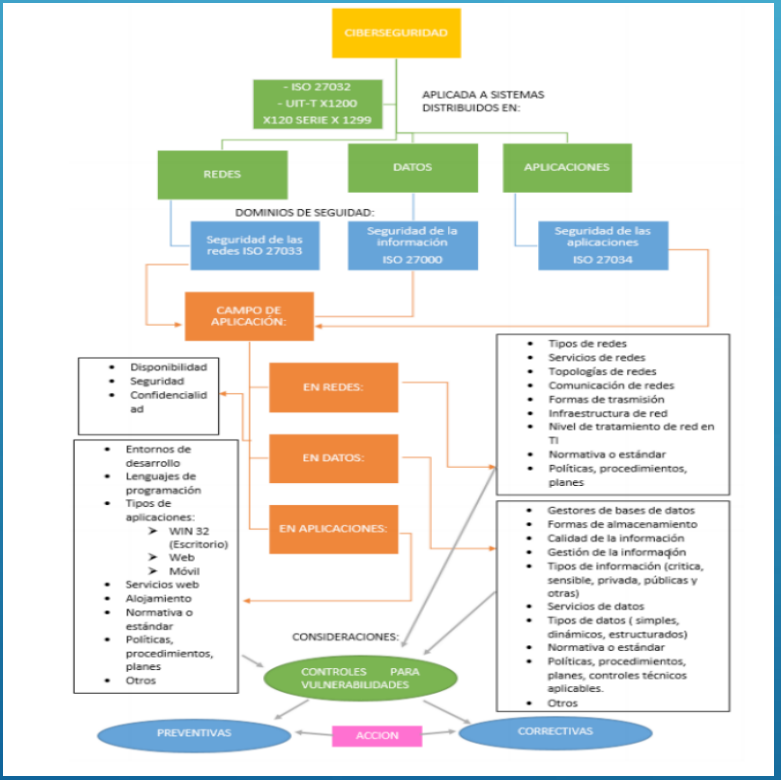
1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

Ciberseguridad



1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

Esquema de Ciberseguridad



1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

El **Instituto Nacional de Ciberseguridad de España** (**INCIBE**) es una sociedad mercantil estatal (S.M.E.) (un tipo de empresa pública) y medio propio (M.P.)[1] organizada como sociedad anónima propiedad del Ministerio de Asuntos Económicos y Transformación Digital de España a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Su denominación social es S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A.

https://www.incibe.es/

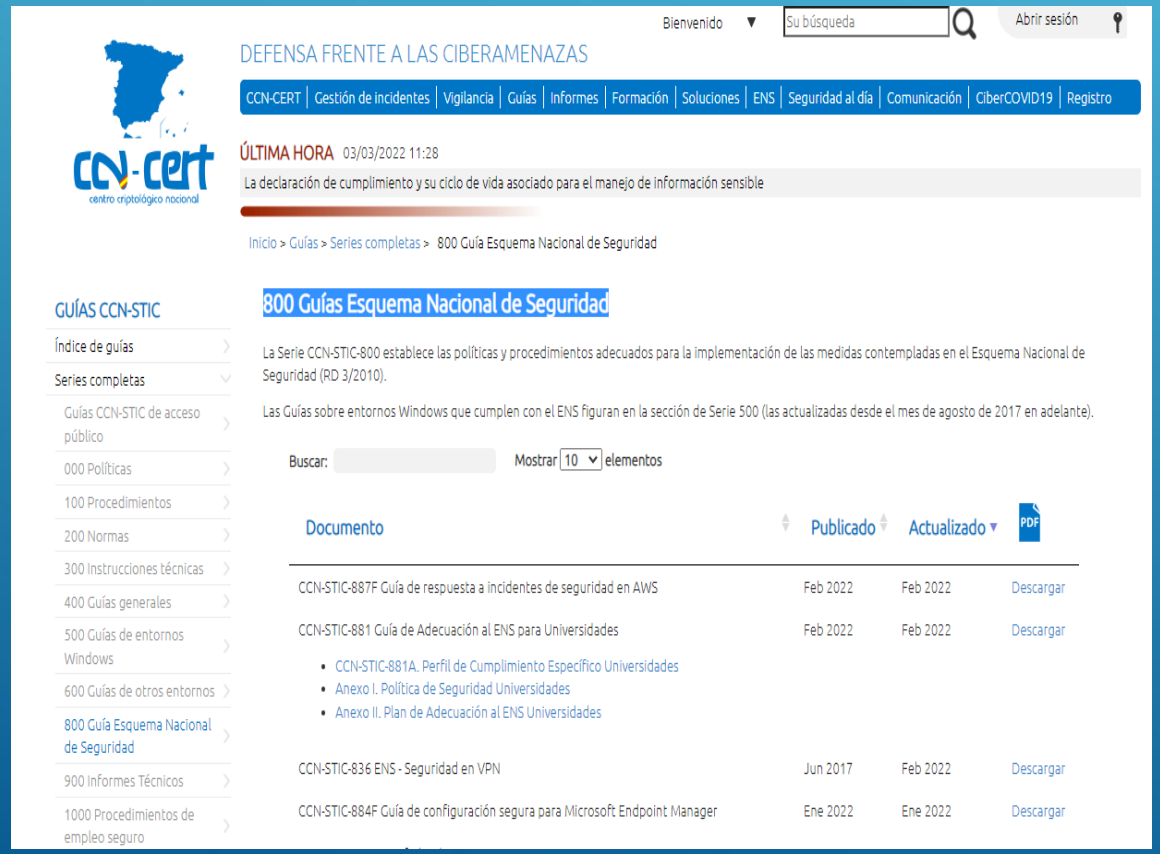
1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

ISO/IEC 27001 Y ENS: DUPLA PARA LA CIBERSEGURIDAD

Es de sobra conocido que la ciberseguridad es transversal a cualquier sistema/tecnología de información utilizada por las organizaciones. Así, dentro de este entorno, se tienen como herramientas básicas para la prevención y defensa en ciberseguridad, el estándar internacional ISO/IEC 27001 de Sistemas de Gestión de la Seguridad de la Información (SGSI) y concretamente en España, el Real Decreto Español 3/2010 por el que se regula el **Esquema Nacional de Seguridad** (ENS).

1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

800 Guías Esquema Nacional de Seguridad



1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

ISO/IEC 27001 Y ENS: DUPLA PARA LA CIBERSEGURIDAD

https://angeles.ccn-cert.cni.es/index.php/es/menu-formacion-es/cursos-online-ccn-ciberseguridad-menu-es#capacitacion-ens

1.4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

ISO/IEC 27001 Y ENS: DUPLA PARA LA CIBERSEGURIDAD