Introducción a la ciberseguridad

"La ciberseguridad es un viaje continuo, no un destino"

Centr@Tec
Servicios Avanzados de Innovación para Pymes

AIR INSTITUTE

icecyl competitividad empresarial

Junta de Castilla y León

Introducción a la ciberseguridad

Introducción.

La ciberseguridad se ha convertido en una necesidad fundamental para todos nosotros.

Como individuos, empresas y sociedad, dependemos cada vez más de la tecnología para nuestras actividades diarias.

Sin embargo, esta dependencia también nos expone a nuevos riesgos y amenazas que debemos comprender y gestionar adecuadamente.

¿Qué es la Ciberseguridad?

La ciberseguridad es el conjunto de prácticas destinadas a proteger equipos, redes, sistemas y datos frente a amenazas digitales.

Su finalidad es preservar tres aspectos clave de la información:

1. La confidencialidad (que solo acceda quien debe)

1. La integridad (que no se altere sin autorización)

1. La disponibilidad (que esté accesible cuando se necesite).

¿Por qué es importante la Ciberseguridad?

Factores críticos

- Protección de la información
- Continuidad del negocio
- Cumplimiento normativo
- Reputación y confianza

Conceptos básicos de ciberseguridad.

Amenazas

Son ataques dirigidos a personas u organizaciones con el objetivo de robar información, causar daños o interrumpir servicios.

Vulnerabilidades

Son debilidades en un sistema que pueden ser aprovechadas por atacantes para comprometer la seguridad.

Riesgo

Es la probabilidad de que una amenaza explote una vulnerabilidad específica y cause daño.

Tipos de ataques más comunes.

Malware

Es un software malicioso diseñado para dañar sistemas o robar información. Incluye virus, troyanos, ransomware y spyware.

Phishing

Es una técnica de suplantación de identidad donde los atacantes se hacen pasar por entidades confiables para robar credenciales o información personal.

Ransomware

Es un tipo específico de malware que cifra los archivos del usuario y exige un rescate para restaurar el acceso.

Ingeniería social

La ingeniería social manipula psicológicamente a las personas para que revelen información confidencial o realicen acciones que comprometan la seguridad.

Medidas de protección.

El Cyber Resilience Act (CRA)

¿Qué es el CRA?

Es una directiva de la Unión Europea destinada a mejorar la seguridad de los productos con elementos digitales, tanto software como hardware.

Esta normativa entró en vigor el 10 de diciembre de 2024.

Se aplica a:

- **Fabricantes** de productos con elementos digitales
- **Importadores** que introducen productos en el mercado europeo
- **Distribuidores** de hardware y software conectado
- **Desarrolladores** de aplicaciones y sistemas

Implicaciones del CRA.

Requisitos obligatorios

- Seguridad por diseño.
- Gestión de vulnerabilidades.
- Actualizaciones de seguridad.
- Documentación técnica.

Plazos de implementación

- Septiembre 2026: Obligaciones de reporte de vulnerabilidades.
- Diciembre 2027: Aplicación completa de todos los requisitos.

Sanciones

Las multas pueden alcanzar hasta 15 millones de euros o el 4% del volumen de negocio anual.

Sello de Confianza

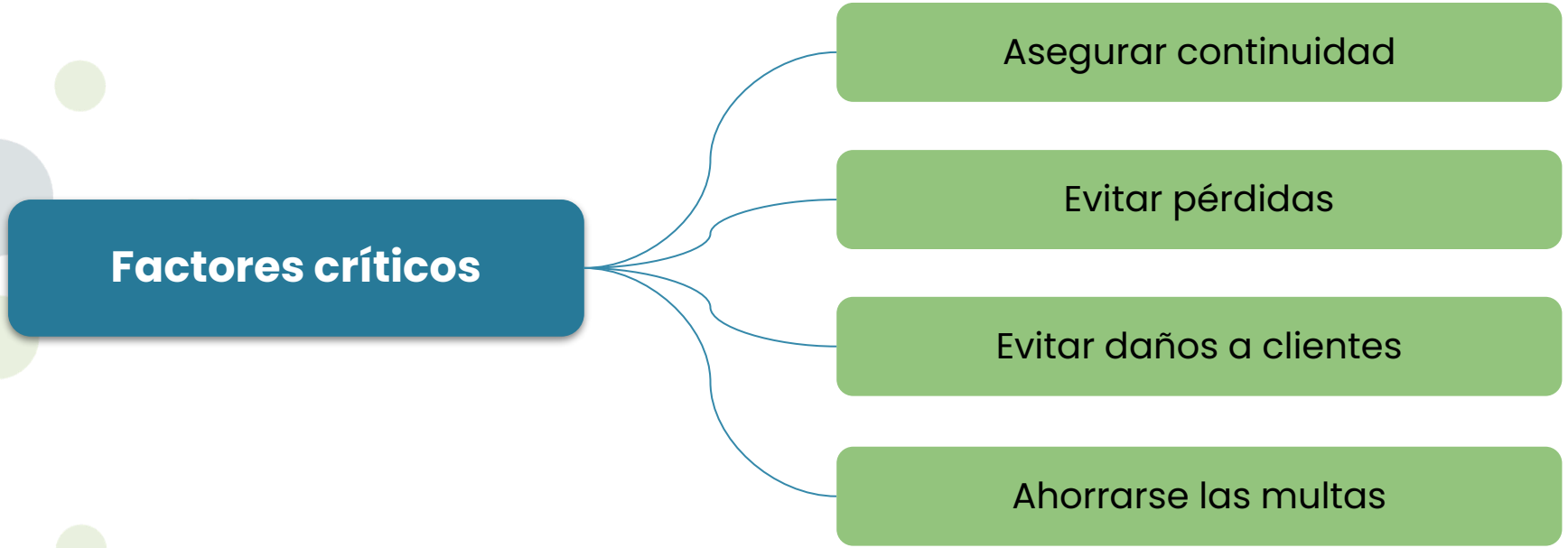
¿Qué es un Sello de Confianza?

Un certificado verificable que demuestra que tu negocio protege datos y sistemas con estándares normativos.

¿Qué es? Una certificación que avala y valida que tus sistemas tecnológicos (digitales y físicos) son seguros y cumplen con las normativas europeas.

¿Por qué importa? Genera confianza instantánea en tus clientes, te destaca en el mercado y abre puertas a nuevos contratos.

¿Por qué invertir en una Certificación?



Proceso del Sello de Confianza

Paso 1

Diagnosticar riesgos con un autodiagnóstico inicial.

Paso 2

Implementar Mejoras

*A veces se podrá hacer una auditoria

Paso 3

Obtén el Sello y muéstralo en tu web o local.

Consecuencias de no tenerlo.

Multas devastadoras: 100s de euros hasta millones o 4% de facturación anual por violar RGPD.

Cierre de operaciones:
Un ataque ransomware puede paralizar tu negocio meses, perdiendo clientes clave.

Pérdida irreparable:
Filtraciones de datos destruyen la confianza, ahuyentando socios y contratos públicos.

Sanciones legales: Responsables enfrentan demandas penales por mala gestión de datos sensibles.

Security Operations Center (SOC)

¿Qué es un SOC?

Un **Security Operations Center (SOC)** es un centro de operaciones de seguridad que funciona como el núcleo de la ciberdefensa de una organización.

Es un equipo centralizado de especialistas en ciberseguridad que operan 24/7 para monitorear, detectar, analizar y responder a amenazas de seguridad en tiempo real.

¿Cómo funciona un SOC?

Componentes clave

- Personas: Analistas de seguridad, ingenieros, especialistas en respuesta a incidentes.
- Procesos: Metodologías estandarizadas para la detección y respuesta.
- Tecnología: Herramientas avanzadas como SIEM, EDR, y sistemas de automatización.

Funciones principales

- Monitorización continua.
- Detección de amenazas.
- Análisis de incidentes.
- Respuesta a incidentes.
- Gestión de vulnerabilidades.

¿Por qué es importante un SOC? Beneficios clave.

- ***Detección temprana***
- ***Respuesta rápida***
- ***Monitoreo continuo***
- ***Cumplimiento normativo***
- ***Reducción de costos***

Ejemplos prácticos.

Caso 1	El phishing que cazó a un empleado
Caso 2	La empresa que se convirtió en referente
Caso 3	Ataques a grandes empresas

Recomendaciones prácticas.

Para individuos

- *Usar contraseñas seguras*
- *Mantener el software actualizado*
- *Ser cautelosos con enlaces y archivos adjuntos*
- *Realizar copias de seguridad*
- *Activar la autenticación multifactorial*

Para empresas

- *Implementar políticas de seguridad*
- *Formar regularmente a los empleados*
- *Mantener inventarios actualizados*
- *Desarrollar planes de respuesta a incidentes*
- *Considerar la implementación de un SOC*

Cierre: La ciberseguridad es una responsabilidad compartida.

La ciberseguridad es una responsabilidad compartida, no solo del área técnica, sino de todos los miembros de una organización y de cualquier persona en el entorno digital.

Aunque las amenazas cibernéticas evolucionan constantemente, con las herramientas, el conocimiento y la actitud adecuados, es posible construir un entorno digital más seguro.

El futuro de la ciberseguridad dependerá de nuestra capacidad de adaptación, del uso de normativas como el CRA y de herramientas como el SOC.

Gracias por su atención