Incidentes de Ciberseguridad – UD1.3

Plan de Formación y Concienciación en Ciberseguridad

IES Chan do Monte – Curso 2025/26
Docente: Simal Paz, Daniel

🧭 Índice

---

1. Introducción

La **ciberseguridad** se define como la protección de los sistemas de información y comunicaciones frente a las amenazas cibernéticas.
En palabras del *Enclave de Ciencia (RAE)*, es la protección de los componentes de las infraestructuras tecnológicas ante ataques o incidentes que puedan comprometer su funcionamiento o la información que contienen.

Un **incidente de ciberseguridad** es un evento inesperado que altera, compromete o daña los sistemas o los datos. Su correcta gestión es clave para garantizar la continuidad operativa y la protección de los activos digitales.

La **ciberseguridad es una responsabilidad compartida**: cada usuario, estudiante o empleado forma parte de la primera línea de defensa. Por ello, un **plan de formación y concienciación** busca capacitar a las personas para identificar amenazas, adoptar hábitos seguros y responder adecuadamente ante incidentes.

📌 *Ejemplo:* un empleado que detecta y reporta un intento de phishing evita una brecha de datos que podría comprometer toda la red corporativa.

---

2. Principios generales en materia de ciberseguridad

2.1 Principios básicos (Modelo CIA y complementarios)

La información —entendida como un conjunto de datos organizados que representan conocimiento — es el activo más valioso de una organización.
Para protegerla, se establecen los **principios básicos de la ciberseguridad**, también conocidos como modelo **CIA**:

Principio	Definición	Ejemplo	Medidas
Confidencialidad	Solo las personas autorizadas pueden acceder a la información.	Acceso restringido a expedientes o datos personales.	Contraseñas robustas, cifrado, MFA.
Integridad	La información no debe alterarse sin autorización.	Modificación no autorizada de registros.	Control de versiones, verificación de hashes.
Disponibilidad	La información debe estar accesible cuando se necesite.	Servidor operativo en horario laboral.	Copias de seguridad, redundancia, UPS.

A estos tres principios se añaden otros dos complementarios:

- **Autenticación:** verificación de la identidad de quien accede.
- **No repudio:** garantía de que ninguna de las partes puede negar su participación en una comunicación.

📌 *Fuente: INCIBE, ENISA.*

Otros principios: autenticación, trazabilidad y no repudio.
📌 *INCIBE – Principios básicos de ciberseguridad*

2.2 Amenaza, vulnerabilidad y riesgo

Concepto	Definición	Ejemplo
Amenaza	Situación o agente capaz de causar daño.	Ciberataque, error humano, malware.
Vulnerabilidad	Debilidad o fallo que puede ser explotado.	Contraseña débil o software desactualizado.
Riesgo	Probabilidad de que una amenaza explote una vulnerabilidad.	Acceso indebido a datos personales.

📌 ENISA – Risk Management Framework

El **riesgo** no puede eliminarse totalmente, pero puede **reducirse** mediante medidas técnicas, organizativas y de concienciación.

2.3 Amenazas a los principios básicos

- **Confidencialidad:** robo o filtración de credenciales.
- **Integridad:** manipulación de datos mediante ataques *man-in-the-middle*.
- **Disponibilidad:** interrupciones del servicio (por ejemplo, ataques DDoS o robo de cableado).

📌 *Ejemplo real:* el ataque de ransomware al SEPE (2021) paralizó servicios públicos durante semanas.

2.4 Medidas para mantener los principios

Principio	Medidas recomendadas
Confidencialidad	Formación en ciberseguridad, cifrado de datos, autenticación multifactor.
Integridad	Protocolos seguros (TLS/SSL), copias de respaldo verificadas.
Disponibilidad	Redundancia de sistemas, medidas físicas de protección, mantenimiento preventivo.

📌 Guía INCIBE – Medidas de Seguridad para PYMEs

---

3. Auditorías de seguridad

Las **auditorías de seguridad** son procesos de verificación del cumplimiento de las medidas de protección.
Permiten identificar puntos débiles, comprobar el cumplimiento normativo (ISO 27001, ENS, RGPD) y establecer mejoras continuas.

- **Auditorías internas:** realizadas por personal de la organización independiente del área TIC.

- **Auditorías externas:** realizadas por terceros certificados; requieren confidencialidad y planificación.

📌 *Referencia: ISO 19011 – Directrices para auditorías.*

Las auditorías comprueban si las medidas de seguridad son eficaces y si cumplen ISO, ENS o RGPD.
📌 *ISO 19011 – Directrices para auditorías*

---

4. Normativa de protección del puesto de trabajo

Norma	Descripción	Ámbito
ISO/IEC 27001	Gestión de la seguridad de la información.	Internacional.
RGPD (UE 2016/679)	Protección de datos personales.	Unión Europea.
ENS (RD 3/2010)	Seguridad de la información en la Administración Pública.	España.
LOPDGDD (Ley Orgánica 3/2018)	Adaptación española del RGPD.	España.

Tabla comparativa:

Norma	Objetivo principal	Entidad	Ejemplo
ISO/IEC 27001	Implementar un Sistema de Gestión de Seguridad (SGSI).	Empresas y organismos.	Empresa TIC certificada.
RGPD	Garantizar derechos de privacidad y protección de datos.	Toda organización que trate datos personales.	Centro educativo.
ENS	Proteger servicios electrónicos públicos.	Administraciones públicas y proveedores.	Ayuntamiento digital.

📌 AEPD

---

5. Factores vulnerables y riesgos en el puesto de trabajo

El puesto de trabajo moderno incluye hardware, software, datos, personas y comunicaciones, tanto en oficina como en teletrabajo.

Factor	Descripción	Ejemplo de riesgo	Prevención
Hardware	Dispositivos físicos.	USB infectado, pérdida de portátil.	Desactivar puertos, cifrado de discos.
Software	Aplicaciones y sistemas.	Instalar software no autorizado.	Uso de software licenciado, actualizaciones.
Personas	Errores humanos o mala praxis.	Contraseñas débiles, phishing.	Formación continua, MFA.
Datos	Información sensible.	Fuga o pérdida de datos.	Cifrado, copias de seguridad.
Comunicaciones	Redes internas y externas.	Uso de WiFi pública sin protección.	VPN, firewalls.

📌 CCN-CERT – Guías STIC

📌 *Fuente: CCN-CERT – Guías STIC.*

---

6. Medidas de seguridad preventivas

Tipo	Descripción	Ejemplo
Preventiva	Evita que ocurra el ataque.	Antivirus, firewalls, formación.
Detectiva	Identifica anomalías.	IDS, SIEM, alertas de red.
Correctiva	Restaura el sistema afectado.	Copias de seguridad, recuperación de sistemas.

📌 INCIBE – Guía de medidas preventivas

📌 *Referencia: INCIBE – Guía de medidas preventivas.*

---

7. Plan de formación y concienciación

7.1 Criterios para el diseño

- Evaluar el nivel de conocimiento del personal.
- Adaptar la formación según roles y responsabilidades.
- Actualizar contenidos ante cambios tecnológicos.
- Incluir simulaciones prácticas y campañas de phishing.
- Medir resultados mediante encuestas y métricas.

📌 *Referencia: INCIBE – Kit de Concienciación.*

📌 *INCIBE – Kit de Concienciación*

7.2 Contenidos de la formación

- Contraseñas seguras y autenticación multifactor.
- Phishing e ingeniería social.
- Uso responsable de Internet y correo electrónico.
- Seguridad en teletrabajo y dispositivos móviles.
- Copias de seguridad y actualizaciones.
- Gestión de incidentes y notificación.
- Protección de datos personales (LOPDGDD).
- Política de “mesa limpia”.

7.3 Elaboración del plan

Elemento	Descripción
Objetivo	Fomentar una cultura de seguridad y reducir incidentes.
Roles	Usuarios, técnicos, dirección.
Metodología	Cursos presenciales, módulos online, carteles, simulacros, correos informativos.
Evaluación	Encuestas, campañas de prueba, informes de incidentes.

📌 CISA – Cybersecurity Awareness Training

📌 *Referencia: CISA – Cybersecurity Awareness Training.*

---

8. Materiales de formación y concienciación

Tipo de material	Ejemplo	Finalidad
Guías y trípticos	“Buenas prácticas con contraseñas”.	Información rápida.
Vídeos	Tutorial sobre phishing.	Aprendizaje visual.
Simulaciones	Ataques de phishing simulados.	Evaluar comportamiento.
Infografías y carteles	Normas básicas de seguridad.	Refuerzo constante.
Encuestas	Cuestionarios de percepción.	Medir efectividad.

📌 INCIBE – Recursos educativos

📌 *Fuentes: INCIBE, ENISA.*

---

9. Recursos y enlaces

- **INCIBE:** www.incibe.es
- **CCN-CERT:** www.ccn-cert.cni.es
- **ENISA:** www.enisa.europa.eu
- **NIST:** www.nist.gov
- **CISA:** www.cisa.gov

---

10. Glosario

Término	Definición	Prevención
Phishing	Correo fraudulento que suplanta identidades.	No abrir enlaces sospechosos.
MFA	Autenticación multifactor.	Combinar contraseña + código.
Backup	Copia de seguridad.	Realizar copias periódicas.
Firewall	Filtro de tráfico.	Configurar reglas seguras.
ENS	Esquema Nacional de Seguridad.	Cumplir revisiones periódicas.

---

11. Conclusiones

La **formación y concienciación** son pilares esenciales de la ciberseguridad.
Las tecnologías protegen, pero **las personas previenen**.
Un plan continuo de capacitación fortalece la resiliencia organizativa, reduce riesgos y garantiza la protección de los datos y sistemas.