Incidentes de Ciberseguridad – UD1.2

Plan de Prevención y Concienciación en Ciberseguridad

IES Chan do Monte – Curso 2025/26

Docente: Simal Paz, Daniel

Normativas de Protección del Puesto de Trabajo

Índice

---

1. Introducción

La protección del puesto de trabajo y la gestión de incidentes de ciberseguridad son pilares esenciales en cualquier plan de prevención.
Cada organización —ya sea una empresa, una administración pública o un centro educativo— está expuesta a amenazas que pueden comprometer sus datos o interrumpir sus servicios.

Un **incidente de seguridad** puede ser tan simple como la pérdida accidental de información o tan grave como un ataque de ransomware que paraliza enteros los sistemas.
Por ello, conocer las **normativas y procedimientos** que regulan la ciberseguridad es clave para saber **cómo actuar, responder y prevenir** .

📌 *Ejemplo:*
Un ayuntamiento sufre la infección de sus servidores por ransomware. Gracias a las directrices del **Esquema Nacional de Seguridad (ENS)** , logra aislar el incidente, restaurar sus copias de seguridad y notificar correctamente al **CCN-CERT** , evitando un daño mayor.

El objetivo de esta unidad es conocer las **principales normativas nacionales e internacionales** que rigen la protección del puesto de trabajo y la gestión de incidentes, así como su aplicación práctica.

---

2. Definición de Incidente de Seguridad

Según la **norma ISO 27001** , un incidente de seguridad de la información es:

> “Un evento o serie de eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones o amenazar la seguridad de la información”.

De forma más sencilla, el **INCIBE** lo define como:

> “Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información”.

🔹 **Ejemplos comunes:**

- Accesos no autorizados a información interna.
- Infecciones por malware o ransomware.
- Pérdida o robo de dispositivos corporativos.
- Phishing dirigido a empleados.
- Fallos de configuración que dejan expuestos datos.

En la mayoría de los casos, **el factor humano** es el origen: contraseñas débiles, desconocimiento o falta de formación en ciberseguridad.

---

3. Normativa de Referencia

Existen diferentes marcos legales y estándares técnicos que sirven de guía para la gestión de incidentes de seguridad.
Entre los más relevantes destacan:

3.1 ISO/IEC 27035 – Gestión de Incidentes de Seguridad

Esta norma internacional forma parte de la familia **ISO/IEC 27000** , que regula la seguridad de la información.
La ISO 27035 establece un **modelo estructurado** para la gestión de incidentes:

1. **Detección y análisis** de eventos de seguridad.
2. **Evaluación** para determinar si un evento es realmente un incidente.
3. **Respuesta y mitigación** proporcional al impacto.
4. **Lecciones aprendidas** para mejorar los procedimientos.

📌 *Recurso:*
ISO 27035 – Gestión de Incidentes de Seguridad

3.2 NIST – Instituto Nacional de Estándares y Tecnología

El **NIST** , dependiente del Departamento de Comercio de EE.UU. UU., desarrolla estándares tecnológicos reconocidos internacionalmente.

En 2013, bajo la orden ejecutiva del presidente Barack Obama, se elaboró el **NIST Cybersecurity Framework (CSF)** , orientado a proteger infraestructuras críticas y reducir los riesgos cibernéticos.

El documento **NIST SP 800-61** (Guía de manejo de incidentes de seguridad informática) proporciona directrices prácticas para el manejo de incidentes:

- **Identificar:** los activos y sus vulnerabilidades.
- **Proteger:** implementar controles adecuados.
- **Detectar:** anomalías y amenazas.
- **Respondedor:** contener y erradicar el incidente.
- **Recuperar:** restaurar los servicios y extraer lecciones aprendidas.

📌 *Recurso:*
Marco de ciberseguridad del NIST

3.3 ENS – Esquema Nacional de Seguridad

El **Esquema Nacional de Seguridad (ENS)** , regulado por el Real Decreto 3/2010 y modificado por el RD 951/2015, establece los principios básicos de la seguridad en la administración electrónica española.

Sus objetivos son:

- Crear **condiciones de confianza** en el uso de medios electrónicos.
- Garantizar la **protección de sistemas, datos y comunicaciones** .
- Definir una política de seguridad aplicable a todas las entidades públicas.

Principios básicos del ENS:

- Seguridad como proceso integral (técnico, humano y organizativo).
- Análisis y gestión continua del riesgo.
- Prevención, detección y recuperación.
- Líneas de defensa en capas.
- Reevaluación periódica de las medidas.
- Roles diferenciados: responsable de la información, del servicio y de la seguridad.

📌 *Recurso:*
Esquema Nacional de Seguridad (ENS)

3.4 CCN-CERT y Guías Nacionales

El **Centro Criptológico Nacional (CCN)** , adscrito al **Centro Nacional de Inteligencia (CNI)** , coordina la respuesta a incidentes de seguridad en el ámbito público a través del **CCN-CERT** .

Guías públicas y herramientas de apoyo, como:

- **CCN-STIC 817 – Gestión de Ciberincidentes.**
- **Guía Nacional de Notificación y Gestión de Ciberincidentes (2020).**

Estas guías definen cómo deben **clasificarse, notificarse y gestionarse los incidentes** , además de los criterios de peligrosidad y obligatoriedad de notificación.

📌 *Recurso:*
Portal CCN-CERT

---

4. Marco Legal Español

La ciberseguridad en España se apoya en un marco regulador amplio que afecta tanto al sector público como al privado:

Leyes generales:

- Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de derechos digitales.
- Real Decreto-ley 12/2018 de seguridad de las redes y sistemas de información.
- Ley 8/2011 de protección de infraestructuras críticas.
- Ley 34/2002 de servicios de la sociedad de la información y comercio electrónico.

Normas específicas:

- Ley 11/2002 del Centro Nacional de Inteligencia.
- Real Decreto 3/2010 del Esquema Nacional de Seguridad.
- Real Decreto 421/2004 que regula el CCN.
- Guías de cumplimiento publicadas por el **Consejo Nacional de Ciberseguridad** .

📌 *Recurso:*
BOE – Legislación sobre Ciberseguridad

---

5. Taxonomía de los Incidentes

La **taxonomía** es la clasificación de los incidentes según su naturaleza, origen o impacto. Permite priorizar la respuesta y analizar patrones.

Ejemplos de categorías comunes:

Tipo de Incidente	Descripción	Ejemplo
Suplantación de identidad (phishing)	Suplantación para obtener credenciales	Correo falso de banco
Malware	Software malicioso que daña sistemas	ransomware o troyano
DDoS	Saturación de un servicio o web	Caída de página institucional
Acceso no autorizado	Intrusión o robo de datos	Robo de contraseñas
Fraude digital	Suplantación o estafa	Phishing corporativo
Ingeniería social	Manipulación psicológica	Falsa llamada del “soporte técnico”

📌 *Recurso:*
ENISA – Taxonomía de clasificación de incidentes de referencia

---

6. Niveles de Peligrosidad e Impacto

Cada incidente se evalúa por su **peligrosidad** (gravedad) y su **impacto** (efecto en la organización).

Ejemplo de niveles de peligrosidad:

- **Crítico:** ataques persistentes avanzados (APT).
- **Alto:** ransomware, intrusiones, pérdida de datos.
- **Medio:** ingeniería social, phishing, vulnerabilidades.
- **Bajo:** spam o escaneo de red.

Ejemplo de niveles de impacto:

- **Crítico:** afecta servicios esenciales o seguridad ciudadana.
- **Alto:** interrupción prolongada o daño reputacional.
- **Medio:** afectación parcial de sistemas.
- **Bajo:** incidencia leve y rápida recuperación.

---

7. Importancia de la Clasificación

Clasificar correctamente los incidentes permite:

- **Priorizar la respuesta** según la gravedad.
- **Asignar recursos eficientemente.**
- **Detectar tendencias y amenazas repetitivas.**
- **Medir la eficacia** de las políticas de seguridad.

Además, ayuda a elaborar informes, alimentar bases de inteligencia y cumplir con los requisitos de notificación ante organismos oficiales.

---

8. Recursos y enlaces

📌 INCIBE – Instituto Nacional de Ciberseguridad
📌 CCN-CERT – Centro Criptológico Nacional
📌 ENS – Esquema Nacional de Seguridad
Marco de ciberseguridad del NIST
📌 ENISA – Agencia Europea de Ciberseguridad

---

9. Glosario de Términos

Término	Definición	Prevención
Suplantación de identidad (phishing)	Suplantación mediante correos o webs falsas.	No abrir enlaces sospechosos, usar MFA.
Malware	Software peligroso o espía.	Antivirus y actualizaciones.
Ransomware	Cifra archivos y exige rescate.	Copias de seguridad.
Cortafuegos	Filtra tráfico no autorizado.	Configuración adecuada.
CCN-CERT	Equipo español de respuesta a incidentes.	Notificar incidentes y aplicar guías STIC.
ENS	Normativa de seguridad pública.	Cumplir roles y evaluaciones periódicas.
VPN	Red privada cifrada.	Usar en redes públicas.
Ingeniería social	Manipulación psicológica.	Verificar identidad antes de actuar.
DDoS	Ataque de saturación de servicios.	Monitoreo y mitigación.
Respaldo	Copia de seguridad.	Realizar copias periódicas.

---

10. Conclusiones

La ciberseguridad no depende solo de las herramientas técnicas, sino del conocimiento y la aplicación de las **normativas que la sustentan** .
Conocer los marcos de referencia como **ISO 27035, NIST, ENS y las guías del CCN-CERT** permite una gestión eficaz, coordinada y proactiva de los incidentes.

Cada trabajador o estudiante tiene un papel fundamental en la **protección del puesto de trabajo digital** .
Cumplir las normas, formarse y actuar con responsabilidad es la mejor forma de prevenir incidentes y construir una cultura de seguridad sólida.