Incidentes de Ciberseguridad – UD1

Plan de Prevención y Concienciación en Ciberseguridad
IES Chan do Monte – Curso 2025/26
Docente: Simal Paz, Daniel

Índice

1. Introducción
2. Objetivos del Plan
3. Líneas de Acción
    - 3.1 Prevención Técnica
    - 3.2 Prevención Organizativa
    - 3.3 Concienciación y Formación
4. Metodología de Implementación
5. Ejemplos de Amenazas Comunes y Cómo Prevenirlas
6. Beneficios Esperados
7. Conclusiones
8. Glosario de Términos Técnicos en Ciberseguridad

---

1. Introducción

Vivimos en una sociedad digitalizada en la que gran parte de nuestras actividades —trabajar, estudiar, comprar, comunicarnos— se desarrollan en Internet. Esta comodidad trae consigo riesgos que afectan a la **seguridad de la información**.

La **ciberseguridad** se ha convertido en una necesidad fundamental. Los incidentes no solo afectan a multinacionales: una pyme, un centro educativo o incluso un usuario particular pueden convertirse en víctimas de un ataque.

Ejemplos reales:

- Una biblioteca municipal que pierde su catálogo por un **ransomware**.
- Un estudiante que comparte sus claves tras caer en un **phishing**.
- Una tienda online caída durante horas por un **ataque DDoS**.

En la mayoría de los casos, el origen de los problemas es el **factor humano**: contraseñas débiles, descargas inseguras o confianza excesiva en correos y mensajes sospechosos.

Por eso, este plan combina **medidas técnicas, organizativas y de concienciación** para reforzar la seguridad desde el punto de vista más importante: **las personas**.

---

2. Objetivos del Plan

El plan de prevención y concienciación busca:

- **Reducir vulnerabilidades** mediante medidas técnicas y organizativas.
- **Aumentar la conciencia de riesgos** en toda la comunidad educativa.
- **Definir protocolos de actuación** frente a incidentes de seguridad.
- **Cumplir con normativas y estándares** (RGPD, ENS, ISO 27001, NIST).
- **Fomentar una cultura de seguridad** como responsabilidad colectiva.

---

3. Líneas de Acción

3.1 Prevención Técnica

Medidas concretas para proteger sistemas y dispositivos:

- **Política de contraseñas seguras** → robustas, únicas y renovadas periódicamente.
- **Actualizaciones y parches** → los atacantes explotan fallos ya conocidos.
- **Copias de seguridad** → permiten recuperar información tras un incidente.
- **Seguridad en red** → firewalls, segmentación de red, control de accesos.

📌 Recurso: Guía de contraseñas seguras – INCIBE

3.2 Prevención Organizativa

Acciones a nivel de gestión:

- **Políticas claras y comprensibles** → que todo usuario sepa qué está permitido y qué no.
- **Clasificación de información** → pública, interna, confidencial, restringida.
- **Protocolos de respuesta a incidentes** → pasos definidos para reportar y actuar.

3.3 Concienciación y Formación

La mejor tecnología falla si las personas no saben usarla correctamente. Ejemplos de actividades:

- **Campañas periódicas** con carteles, charlas y recordatorios.
- **Simulacros de phishing** controlados para entrenar la detección.
- **Talleres prácticos** sobre seguridad en móviles, redes sociales y Wi-Fi.
- **Formación gamificada**: juegos, concursos, retos de seguridad.

📌 Recurso: ObservaCiber – Cómo se protege la ciudadanía

---

4. Metodología de Implementación

El plan debe aplicarse paso a paso:

1. **Diagnóstico inicial**: auditorías, encuestas y simulaciones.
2. **Definición del plan**: objetivos, responsables, calendario.
3. **Ejecución por fases**:
    - Mes 1 → contraseñas seguras.
    - Mes 2 → simulacro de phishing.
    - Mes 3 → seguridad en móviles.
4. **Evaluación**: indicadores como nº de incidentes, participación en formaciones.
5. **Mejora continua**: revisión anual para adaptarse a nuevas amenazas.

---

5. Ejemplos de Amenazas Comunes y Cómo Prevenirlas

Amenaza	Descripción	Prevención
Phishing	Correos o webs falsas que roban credenciales.	No abrir enlaces sospechosos, verificar remitente.
Ransomware	Malware que cifra archivos y exige un rescate.	Backups periódicos, actualizaciones, antivirus.
Wi-Fi pública insegura	Redes abiertas que permiten robo de información.	Evitar operaciones sensibles, usar VPN.
Ingeniería social	Manipulación psicológica para obtener datos o acceso.	Formación, verificación de identidad antes de dar información.

📌 Recurso: INCIBE – Ransomware: cómo protegerse

---

6. Beneficios Esperados

- Menos incidentes de seguridad relacionados con errores humanos.
- Mayor confianza en la institución.
- Cumplimiento de normativas y estándares.
- Cambio cultural: todos somos parte de la ciberseguridad.

---

7. Conclusiones

La ciberseguridad no depende solo de firewalls o antivirus. Se trata de **personas, procesos y tecnología** trabajando juntas.

Un plan de concienciación:

- Protege la información.
- Refuerza la reputación de la organización.
- Prepara a las personas para responder de forma adecuada.

---

8. Glosario de Términos Técnicos en Ciberseguridad

Término	Definición	Ejemplo	Prevención
Phishing	Engaño mediante correos, SMS o webs falsas.	Correo falso del banco pidiendo verificar cuenta.	No abrir enlaces sospechosos, MFA.
Malware	Software malicioso que daña o espía.	Archivo adjunto con spyware.	Antivirus actualizado, precaución con adjuntos.
Ransomware	Cifra archivos y pide rescate.	WannaCry (2017).	Backups, actualizaciones.
Firewall	Filtra tráfico de red.	Bloqueo de accesos no autorizados.	Configuración adecuada.
MFA	Autenticación multifactor.	Contraseña + código SMS.	Activar en servicios críticos.
Cifrado	Convierte datos en ilegibles sin clave.	WhatsApp cifrado extremo a extremo.	Usar HTTPS, TLS, discos cifrados.
VPN	Red privada virtual cifrada.	Conexión segura a la empresa.	Usar en redes públicas.
Exploit	Código que aprovecha vulnerabilidades.	Fallo en Windows sin parchear.	Instalar parches.
Backup	Copia de seguridad de datos críticos.	Backup diario en nube cifrada.	Copias periódicas y restauración.
Ingeniería social	Manipulación psicológica.	Suplantación de técnico de soporte.	Verificar identidad, formación.
Botnet	Red de dispositivos infectados.	Routers usados para spam.	Actualizaciones, contraseñas fuertes.
DDoS	Ataque que sobrecarga un servicio.	Caída de web por saturación.	Mitigación DDoS, monitorización.
Spyware	Programa espía.	App que registra teclas.	Revisar permisos, antimalware.
Troyano	Malware camuflado como legítimo.	Juego que instala malware bancario.	Descargar de fuentes confiables.

Término	Definición	Ejemplo	Prevención
Gusano	Malware que se propaga automáticamente.	Correo infectado replicándose.	Parches de seguridad, antivirus.