Incidentes de Ciberseguridad – UD1.5

Materiales de Formación y Concienciación en Ciberseguridad

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

Índice

---

1. Introducción

Los **materiales de formación y concienciación en ciberseguridad** son el "vehículo" que transforma políticas y buenas prácticas en comportamientos cotidianos. Su eficacia depende tanto del **contenido** como del **formato** (claridad, visualidad, repetición y participación).

Ejemplo claro y concreto

Colocar en zonas visibles un cartel "**Cómo detectar un correo de phishing**" (remitente, enlaces, ortografía, urgencia inusual) reduce clics en enlaces fraudulentos y **aumenta** los reportes de intentos de suplantación.

💡 **Ejemplo:**

Un cartel sobre "Cómo detectar un correo de phishing" colocado en una sala de profesores puede reducir notablemente los clics en enlaces fraudulentos.

📌 *Recurso:* INCIBE – Kit de Concienciación

---

2. Objetivos de los materiales de concienciación

Objetivo general: ayudar a que las personas **reconozcan amenazas**, **actúen correctamente** ante incidentes y **consoliden hábitos** seguros.

Los materiales deben lograr que los usuarios:

- **Reconozcan las amenazas** más comunes.
- **Actúen correctamente** ante incidentes.
- **Incorporen hábitos seguros** en su día a día.
- **Difundan la cultura de ciberseguridad** entre compañeros.

Objetivos específicos

- Reconocer señales de alarma frecuentes (phishing, smishing, adjuntos sospechosos).
- Saber **cómo reportar** y a quién acudir; seguir un **procedimiento** sencillo.
- **Integrar hábitos**: bloqueo de pantalla, actualizaciones, contraseñas robustas y MFA.
- **Reforzar la cultura** de seguridad con mensajes breves, repetidos y atractivos.

📌 *Recurso:* ENISA – Awareness Raising Toolkit

---

3. Tipos de materiales y ejemplos prácticos

3.1 Guías y manuales

Qué son: Documentos (PDF/ODT/DOCX) que explican **normas y procedimientos** con detalle.
Ejemplos concretos

- Guía de **contraseñas seguras + MFA** con capturas de configuración.
- Procedimiento de **notificación de incidentes** (pasos, tiempos y contactos).
  Ventajas: profundidad y trazabilidad. **Desventajas**: menor impacto visual.

3.2 Infografías y carteles

Qué son: Representaciones **visuales** simples y directas, de 1 página.
Ejemplos concretos

- Infografía "**10 señales de un correo sospechoso**".
- Cartel "**Bloquea tu pantalla** y no compartas contraseñas".
  Ventajas: alto impacto y recuerdo. **Desventajas**: requieren diseño.

3.3 Vídeos y material multimedia

Qué son: Piezas **cortas** (1–3 min) con ejemplos reales y llamadas a la acción.
Ejemplos concretos

- Vídeo "**Phishing en 90 segundos**: 3 claves para detectarlo".
- Tutorial de **configuración segura** en móviles y portátiles (actualizaciones, PIN, cifrado).
  Ventajas: didácticos y memorables. **Desventajas**: producción y edición.

3.4 Simulaciones y juegos de rol

Qué son: Actividades **prácticas** que entrenan decisiones y respuestas.
Ejemplos concretos

- Campaña de **phishing simulado** con métricas de **clic** y **reporte**.
- Juego de rol: respuesta ante **ransomware** (aislar, comunicar, restaurar).
  Ventajas: aprendizaje experiencial. **Desventajas**: planificación y recursos.

3.5 Plataformas de e-learning

Qué son: Entornos con cursos, **cuestionarios**, seguimiento y **reportes**.
Ejemplos concretos

- Módulos por niveles (básico/avanzado) + evaluaciones periódicas.
- Integración con campañas de **phishing simulado** y recordatorios.
  Ventajas: trazabilidad y métricas. **Desventajas**: administración y soporte.

---

4. Tabla comparativa de tipos de materiales

Tipo	Formato	Objetivo principal	Público objetivo	Ventaja destacada
Guías	PDF/ Documento	Explicar normas y procedimientos	Todo el personal	Claridad y profundidad
Infografías	Imagen/Póster	Reforzar conceptos clave	Estudiantes y docentes	Alto impacto visual
Vídeos	Multimedia	Mostrar ejemplos reales	Público general	Alta didáctica
Simulaciones	Actividad práctica	Evaluar reacciones y entrenar respuesta	Empleados y técnicos	Entrenamiento realista
E-learning	Plataforma web	Formación continua y seguimiento	Toda la organización	Control del progreso

📌 *Recurso:* MetaCompliance – Security Awareness Resources

5. Cómo crear un programa de materiales eficaz (fases)

Para diseñar un programa de materiales de concienciación se deben seguir estas fases:

Fase	Descripción	Herramientas
1. Análisis de necesidades	Identificar amenazas y nivel de conocimiento.	Encuestas, entrevistas.
2. Diseño de materiales	Seleccionar formatos adecuados.	Canva, Piktochart, PowerPoint.
3. Implementación	Distribuir los materiales periódicamente.	Correo interno, intranet, cartelería.
4. Evaluación	Medir el impacto mediante indicadores.	Cuestionarios, simulaciones.

Fase 1 – Análisis de necesidades

- Encuestas y entrevistas para medir nivel de partida y riesgos prioritarios.
- Identificar **públicos** (alumnado, docentes, PAS, dirección) y mensajes clave.

Fase 2 – Diseño de materiales

- Seleccionar **formatos** (guías, infografías, vídeos, simulaciones).
- Plan editorial trimestral/mensual (temas, responsables, fechas).
- Herramientas útiles: Canva, PowerPoint, Piktochart, plataformas LMS.

Fase 3 – Implementación

- Difusión por **intranet**, correo, pantallas, cartelería y tutorías.
- Ritmo recomendado: **1 pieza/semana** (p. ej., infografía de lunes + microvídeo de jueves).

Fase 4 – Evaluación

- Métricas: tasa de **clic** en phishing simulado, **reporte** de incidentes, finalización de cursos, aciertos en cuestionarios, tiempos de respuesta.
- Mejoras continuas: reforzar los temas con peor desempeño y repetir mensajes clave.

💡 *Ejemplo práctico:*
Un instituto lanza una campaña mensual con infografías y vídeos sobre buenas prácticas digitales. Resultado: mejora del 50 % en la detección de correos fraudulentos entre alumnos y docentes.

📌 *Recurso:* usecure – Security Awareness Training

---

6. Recursos gratuitos recomendados (con hipervínculos)

- **INCIBE – Kit de Concienciación**: https://www.incibe.es/empresas/formacion/kit-concienciacion
- **ENISA – Awareness Raising Materials**: https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-raising
- **Proofpoint – Cybersecurity Awareness Kit**: https://www.proofpoint.com/es/resources/awareness-materials/cybersecurity-awareness-kit
- **MetaCompliance – Awareness Resources**: https://www.metacompliance.com/es/resources/
- **usecure – Security Awareness Training (ideas y ejemplos)**: https://blog.usecure.io/es/cuales-son-los-buenos-ejemplos-de-formacion-en-materia-de-seguridad
- **IS4K – Internet Segura for Kids**: https://www.is4k.es/

Todos los enlaces están pensados para obtener **materiales listos** (pósteres, guías, vídeos, plantillas) que puedas adaptar al centro.

---

7. Recomendaciones para centros educativos

- **Lenguaje y contexto**: adaptar el tono al nivel del alumnado y del profesorado.
- **Curricularización**: integrar los materiales en **tutorías** y proyectos de centro.
- **Simulaciones formativas**: phishing simulado con enfoque **educativo** y métricas.
- **Gamificación**: retos, puntos y rankings (por clases o departamentos).
- **Calendario visible**: “Tema del mes” (p. ej., contraseñas en octubre, privacidad en noviembre…).
- **Alianzas**: aprovechar talleres y recursos de **INCIBE** e **IS4K**.

📌 *Recurso:* Internet Segura for Kids (IS4K)

8. Glosario ampliado

Término	Definición	Aplicación / Ejemplo
Phishing simulado	Ejercicio de prueba para medir la reacción ante correos falsos.	Simulación interna.
Gamificación	Uso de dinámicas de juego para enseñar.	Puntos, logros y recompensas.
E-learning	Formación a distancia mediante plataformas digitales.	Cursos online de seguridad.
Kit de concienciación	Conjunto de materiales educativos en seguridad.	Herramientas de INCIBE.
Microlearning	Formación breve y repetitiva.	Vídeos cortos de 2 minutos.
Awareness program	Programa integral de concienciación.	Plan anual de formación.
Cultura de seguridad digital	Conjunto de hábitos y valores de seguridad.	Conducta responsable en redes.
Ingeniería social	Manipulación psicológica para obtener información.	Llamadas fraudulentas.
VPN	Red privada virtual para conexiones seguras.	Teletrabajo seguro.
Backup	Copia de seguridad de datos.	Almacenamiento externo.

- **Phishing simulado**: ejercicio controlado para medir reacción ante correos falsos.
- **Gamificación**: uso de dinámicas de juego (puntos, logros, recompensas) para aprender.
- **E-learning**: formación a distancia mediante plataforma digital con seguimiento.
- **Kit de concienciación**: conjunto de materiales (pósteres, guías, vídeos, plantillas).
- **Microlearning**: cápsulas de 1–3 minutos que se repiten en el tiempo.
- **Cultura de seguridad digital**: hábitos compartidos que reducen riesgos cotidianos.
- **Ingeniería social**: manipulación para obtener información o accesos.
- **VPN**: red privada virtual para conexiones seguras desde fuera del centro.
- **Backup**: copia de seguridad periódica de datos críticos.

---

9. Conclusiones

Los **materiales de concienciación** conectan la teoría con la práctica y ayudan a convertir **buenas prácticas** en **hábitos**.
Combinar **guías** (profundidad), **infografías** (impacto), **vídeos** (memoria) y **simulaciones** (entrenamiento) genera un programa equilibrado.
La clave es la **constancia** y la **medición**: reforzar lo que peor funciona, repetir los mensajes clave y celebrar los progresos.