CURSO DE ESPECIALIZACIÓN DE CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

INCIDENTES DE SEGURIDAD

Tarea Modulo 1

Desarrollo de Planes de Prevención y Concienciación en Ciberseguridad

Autor: Valentín Fernández Guijarro

Tutor: María Dolores Jiménez Cortés

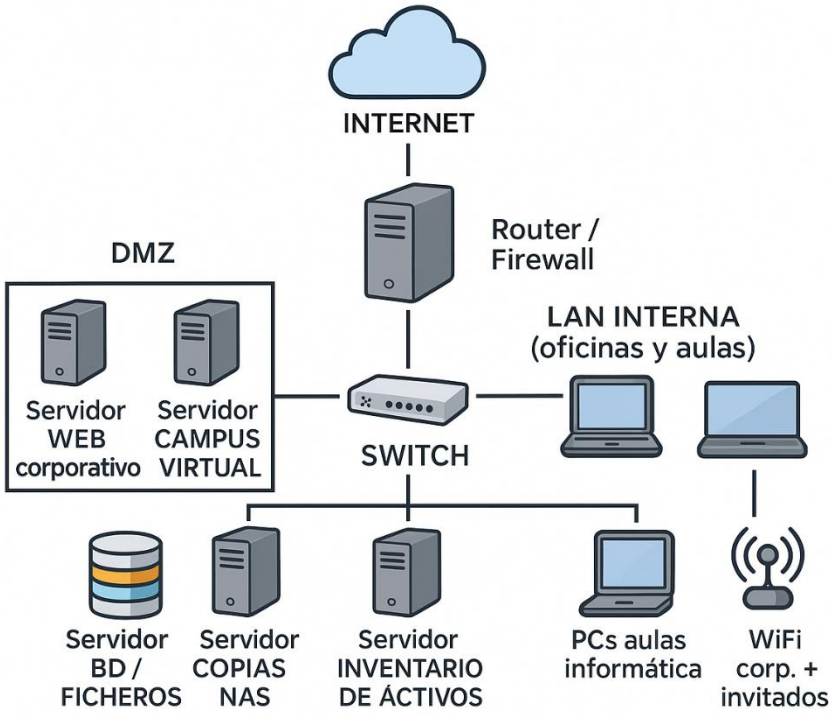
Curso: 2025/2026

INDICE

Apartado 1: Diseño de una Empresa Ficticia o descripción de una existente

Partimos de una academia, AULASUR, cuyo principal campo de formación son las Tecnologías de la información (Desarrollo web, ciberseguridad básica, programación, ofimática, competencias digitales para la empresa), impartiéndose tanto de forma presencial en su única sede en Sevilla o a través de un campus online. Imparte principalmente cursos subvencionados por organismos públicos (SEPE, Junta de Andalucía, Ayuntamientos…) dirigida a personas desempleadas, trabajadores en activo y empresas.

Identificación de activos



Hardware: router/firewall perimetral, switch LAN, servidores (WEB, Campus Virtual, BD/Ficheros, NAS copias, Inventario de activos), PCs de aulas, portátiles, Wi-Fi corporativa/invitados, móviles (BYOD), dispositivos USB.

Software: sistemas operativos, software de seguridad (antivirus, firewall, EDR), software de producción (web, campus, BD), software de gestión (copias, inventario), aplicaciones de usuario (ofimática, navegador, correo) y licencias/propiedad intelectual.

Comunicaciones: conexión a Internet, LAN interna, DMZ (servidor web y campus), Wi-Fi corporativa e invitados, VPN para teletrabajo.

Instalaciones: oficinas, aulas, puestos de trabajo, sala de servidores (CPD), archivadores cerrados y armarios ignífugos.
Datos: bases de datos de negocio, contenidos del campus, datos personales (alumnos, empleados, terceros), inventario de activos, copias de seguridad.

Personas: empleados, docentes, alumnos, dirección, personal técnico, usuarios invitados y terceros (clientes/organismos públicos/proveedores).

Apartado 2: Detalle de los materiales de formación y concienciación del puesto de trabajo que se deberán tener en cuenta.

HARDWARE

Elementos: PCs de aulas, portátiles y equipos de oficina

Escenario H1: Infección por malware a través de memorias USB o descargas. Los alumnos o empleados conectan USB o ejecutan ficheros maliciosos.

Material: Ataque simulado con memorias USB infectadas, Recurso formativo del Kit del INCIBE "El puesto de trabajo. Medidas de protección I y II" (PPT, PDF y test), Posters y consejos del Kit con mensajes del tipo: *"No conectes dispositivos USB de origen desconocido"*.

Escenario H2: Pérdida o robo de portátil sin cifrado. Portátil de la empresa con acceso a correo, campus e información interna que se pierde o roba.

Material: Guía PDF "Buenas prácticas con portátiles", difundida por intranet y correo. Recordatorio en sesiones de formación general.

Escenario H3: Equipos sin bloquear en aulas y oficinas. Sesiones abiertas en aulas/oficinas, pantallas visibles, riesgo de accesos no autorizados.

Material: Posters en aulas y oficinas: *"Bloquea tu equipo antes de levantarte (Win+L)"*.

Elemento: Servidores internos (incluido el servidor de inventario de activos)

Escenario H4: Acceso indebido al inventario de activos y a servidores internos. Configuraciones débiles o credenciales mal gestionadas que permiten a un atacante acceder al inventario o a servidores críticos.

Material: Sesión técnica "Ataque a un inventario de activos", mostrando el impacto real de su compromiso. Recurso del Kit de concienciación del INCIBE sobre "La información como activo" para reforzar la importancia de proteger el inventario como información crítica.

SOFTWARE

Elemento: Sistemas operativos y software de seguridad (antivirus, firewall, EDR)

Escenario S1: – Falta de actualización de sistemas. sistemas desactualizados que mantienen vulnerabilidades conocidas.

Material: Hoja/infografía con el Decálogo de ciberseguridad adaptado a AULASUR enfocándolo en actualizaciones, copias de seguridad y uso de antivirus. Sesión interna para personal técnico sobre gestión de actualizaciones y ciclo de vida de vulnerabilidades.

Escenario S2: Desactivación voluntaria de antivirus o firewall por parte de usuarios. El usuario desactiva temporalmente las protecciones para acelerar el equipo o instalar software.

Material: Vídeo corto explicando el papel del antivirus y ejemplos de incidentes derivados de su desactivación. Banner o mensaje recordatorio en intranet/campus: *"El antivirus es obligatorio. Desactivarlo pone en riesgo a toda la organización"*.

Elemento: Aplicaciones de usuario (correo, navegador, ofimática)

Escenario S3: Phishing y ejecución de adjuntos o enlaces maliciosos. Usuarios que abren adjuntos o hacen clic en enlaces fraudulentos (phishing, smishing, spear phishing).

Material: Campañas simuladas de phishing con Gophish y ataques con enlace malicioso del Kit, antes y después de la formación. "El correo electrónico. Principales fraudes y riesgos" (PPT, PDF, test, posters y consejos) del kit del INCIBE impartido a todo el personal.

Escenario S4: Instalación de software no autorizado o sin licencia.- Usuarios instalan programas no aprobados, con riesgo de malware o incumplimiento legal.

Material: Documento de "Normas de uso de software en AULASUR" (parte de la normativa de puesto de trabajo) distribuido por correo y disponible en intranet. Breve test online para asegurar que el personal ha leído y comprendido las normas.

COMUNICACIONES

Elemento: Internet, LAN interna y DMZ

Escenario C1: Exposición excesiva de servicios en DMZ y ataques desde Internet. Servidores web/campus con servicios innecesarios expuestos, configuraciones débiles o sin endurecer.

Material: Taller con personal técnico sobre estructura en trípode y DMZ segura. Checklist técnico de revisión periódica para servicios expuestos.

Escenario C2: Navegación por sitios maliciosos o de riesgo. usuarios que acceden a webs de descarga ilegal, páginas fraudulentas o poco fiables.

Material: Infografía y consejos del Kit adaptados a "Navegación segura en la empresa", difundidos por correo y en intranet. Breve módulo en el campus con ejemplos de webs peligrosas y cómo identificarlas.

Elemento: Wi-Fi corporativa, red de invitados y VPN

Escenario C3: Uso indebido de la Wi-Fi corporativa con dispositivos personales. Conexión de dispositivos no autorizados a la red interna, con riesgos de malware y fugas.

Material: Cartelería junto a puntos de acceso indicando redes disponibles (empleados / invitados) y normas de uso. Ficha PDF con la política de uso de Wi-Fi corporativa y de invitados.

Escenario C4: Teletrabajo sin VPN o en redes públicas inseguras. Acceso al correo o sistemas corporativos desde redes Wi-Fi públicas sin cifrado adecuado.

Material: Recurso formativo del Kit "Dispositivos móviles y teletrabajo. Riesgos y protección" (PPT, PDF, test). Guía paso a paso para configurar y usar la VPN corporativa, difundida a todo el personal en teletrabajo.

INSTALACIONES

Elemento: Oficinas, aulas, CPD y archivadores

Escenario I1: Documentos confidenciales abandonados en mesas o impresoras. listados de alumnos, nóminas, contratos, etc., que se quedan visibles o en bandejas de impresión.

Material: Posters del Kit sobre "limpieza de mesa" y "protección del papel", colocados en zonas de impresión y puestos sensibles. Instrucciones resumidas en la normativa de puesto de trabajo y recordatorio en sesiones de acogida.

Escenario I2: Acceso por personal no autorizado y no controlado a sala de servidores (CPD) o a archivadores

Material: Procedimiento escrito de acceso físico al CPD (quién, cuándo, cómo, registro) explicado en una sesión específica al personal autorizado. Indicadores visuales en archivadores/armarios con el nivel de sensibilidad de la información y obligación de mantenerlos cerrados.

Escenario I3: Shoulder surfing (miradas indiscretas a la pantalla). Terceros pueden ver información sensible en pantalla (aula, recepción, despacho).

Material: Inclusión de este riesgo en los módulos sobre "El puesto de trabajo. Medidas de protección", con ejemplos prácticos. Recomendaciones sobre ubicación de pantallas y uso de filtros de privacidad.

DATOS

Elemento: Información corporativa y datos personales

Escenario D1: Envío de datos personales sin cifrar o a destinatarios incorrectos

Material: Recurso del Kit sobre clasificación de la información y cifrado (presentación, PDF, test), aplicado a ejemplos reales de AULASUR. Ficha operativa "Qué datos puedo enviar por correo y cómo" (uso de CCO, cifrado de adjuntos, mínimos necesarios).

Escenario D2: Falta de clasificación/cifrado de información sensible. Documentos y ficheros críticos sin etiquetado ni medidas de protección.

Material: Taller práctico donde se realizan ejercicios de clasificación de información usando casos reales (Publicos, Uso interno, Restringido, Confidencial). Plantillas de clasificación y ejemplos disponibles en la intranet.

Escenario D3:_ Copias de seguridad insuficientes o mal gestionadas. No se realizan copias con la frecuencia adecuada, no se prueban las restauraciones o se guardan sin cifrar.

Material: Recurso del Kit "Backups, borrado y tipos de almacenamiento" para personal técnico y de gestión. Mini-sesión específica con dirección explicando el impacto de no disponer de copias funcionales y las responsabilidades asociadas. Explicar regla del 3-2-1

Elemento: Perfiles de redes sociales y web corporativa

Escenario D4: Publicación de información sensible o inadecuada. Publicación de datos personales, imágenes comprometidas o información interna en redes sociales.

Material: Recurso del Kit “Redes sociales. Medidas de seguridad para perfiles de empresa” adaptado a la realidad de AULASUR. Guía breve para el personal que gestiona redes sociales, con ejemplos de contenidos permitidos y prohibidos.

Escenario D5: Suplantación de identidad y ataques reputacionales. Creación de perfiles falsos o uso indebido del nombre de la organización.

Material: Sesión de sensibilización para comunicación/marketing sobre detección de perfiles falsos y reacción ante crisis reputacionales.

PERSONAS

Elemento: Empleados, docentes y alumnos

Escenario P1: Ingeniería social y phishing (correos, llamadas, mensajes). ataques que buscan engañar al usuario para que entregue credenciales o ejecute malware.

Material: Campañas simuladas de phishing (Gophish) y ataques con enlace malicioso, con informe de resultados y refuerzo posterior. Recurso formativo del Kit sobre fraudes por correo con ejemplos y test de evaluación.

Escenario P2: Uso de contraseñas débiles o reutilizadas. Contraseñas simples, compartidas o repetidas entre servicios.

Material: Recurso del Kit “Contraseñas y medidas complementarias” (PPT, PDF, test y consejos). Infografía interna con recomendaciones: longitud mínima, complejidad, no reutilización, uso de segundo factor donde sea posible.

Escenario P3: Desconocimiento de las políticas y falta de cultura de ciberseguridad. el personal no percibe la seguridad como parte de su trabajo diario.

Material: Curso troncal anual de concienciación (basado en el decálogo, normativa de puesto de trabajo y recursos del Kit) obligatorio para todo el personal. Boletín interno de ciberseguridad con secciones de noticias, casos reales, análisis y consejos, enviado periódicamente.

Elemento: Dirección, personal técnico y terceros

Escenario P4: Falta de liderazgo en ciberseguridad por parte de la dirección. Ausencia de mensajes claros desde la dirección, priorización exclusiva del negocio frente a la seguridad.

Material: Sesión ejecutiva breve para dirección, centrada en riesgos, responsabilidades y beneficios de la ciberseguridad. Inclusión periódica de mensajes de la dirección en los boletines y campañas de concienciación.

Escenario P5: Proveedores y colaboradores que tratan datos o acceden a sistemas sin formación adaptada con las políticas de AULASUR

Material: Documento de bienvenida para proveedores con resumen de políticas básicas de ciberseguridad de AULASUR. Cláusulas específicas en contratos y acuerdos de colaboración que se explican y firman.

Apartado 3: Detalle del plan de formación y concienciación.

Objetivos del plan de formación y concienciación

El objetivo general del Plan de formación y concienciación de AULASUR es desarrollar y mantener una *cultura de ciberseguridad* en toda la empresa, de manera que todas las personas que usan los sistemas de información conozcan y apliquen en su puesto de trabajo las medidas necesarias para proteger la *confidencialidad, integridad y disponibilidad* de la información, para ello nos basaremos en la norma ISO 27001 y el Kit de concienciación del INCIBE principalmente.

Evaluación de las necesidades de formación.

Basándonos en los escenarios identificados en el apartado anterior se podrían identificar las siguientes necesidades de formación:

- *Uso seguro del puesto de trabajo y equipos:* Riesgo de malware por USB, portátiles sin proteger, equipos sin bloquear, documentos en impresoras o mesas (escenarios H1, H2, H3, I1, I3).
- *Protección frente a phishing e ingeniería social:* Exposición de los usuarios a correos fraudulentos y enlaces maliciosos (S3, P1).
- *Gestión de contraseñas:* Contraseñas débiles, reutilizadas o compartidas, que comprometen múltiples sistemas (P2).
- *Protección de la información y datos personales: E*nvíos sin cifrar, ausencia de clasificación y uso incorrecto del correo para datos sensibles (D1, D2).
- *Gestión de copias de seguridad y continuidad:* Conocimiento limitado sobre backups, pruebas de restauración y regla 3-2-1 (D3).
- *Uso seguro de redes, Wi-Fi y teletrabajo:* Navegación insegura, uso inapropiado de la Wi-Fi corporativa y accesos remotos sin VPN (C2, C3, C4).
- *Seguridad física y redes sociales:* Accesos físicos no controlados, pantallas expuestas y uso inadecuado de redes sociales corporativas (I2, D4, D5).

Roles incluidos (concreción del plan)

El plan debe estar clasificado por roles de acuerdo con los niveles de complejidad y alcance del control definidos (Básico/Avanzado y Procesos/Tecnología/Personas).

- Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- Procesos (**PRO**): aplica a la dirección o al personal de gestión.
- Tecnología (**TEC**): aplica al personal técnico especializado.
- Personas (**PER**): aplica a todo el personal.

NIVEL	ALCANCE	CONTROL
A	PRO	**Detallar los elementos clave que queremos que sean auditados.** Tienes identificados los activos más relevantes que deben ser auditados.
B	PRO	**Mejora continua y modelos de madurez. m**Enfocas el proceso de auditoría desde un punto de vista de mejora continua o de consecución de niveles de madurez.
A	PRO/TEC	**Auditorías legales.** Realizas auditorías específicas para verificar el cumplimiento de los requerimientos legales del RGPD.
A	PRO/TEC	**Auditorías forenses.** Realizas auditorías forenses para determinar lo ocurrido tras un incidente de seguridad.
A	TEC	**Procedimientos.** Has definido/revisado procedimientos detallados para auditar la seguridad de cada activo clave de tus sistemas de información.
A	TEC	**Realización de auditorías periódicas.** Realizas auditorías de tus sistemas de información de forma periódica.
A	PRO/TEC	**Análisis del resultado de la auditoría.** Analizas los resultados de la auditoría en busca de debilidades a corregir.

Contenidos (de la formación y los criterios) y Asociación de roles y contenidos (adecuados a los distintos puestos de trabajo).

Los contenidos del plan se estructuran en nueve módulos, adaptados con los recursos del Kit de concienciación del INCIBE y con los escenarios de riesgo definidos anteriormente.

Módulo 1. La información: el activo imprescindible de AULASUR

Nivel: B

Alcance: PRO / PER

Contenidos

- La información como activo crítico en AULASUR (datos de alumnos, contenidos del campus, información económica, etc.).
- Conceptos de confidencialidad, integridad y disponibilidad.
- Impacto de la pérdida, filtración o indisponibilidad de la información.

Criterios

- El participante identifica ejemplos de información crítica de AULASUR.
- Es capaz de explicar, en términos sencillos, por qué la información es un activo y qué consecuencias tendría su pérdida.

Roles (PRO/TEC/PER)

- PRO: Dirección y responsables de área.
- PER: Todo el personal y en versión resumida a alumnos.

Módulo 2. La información: clasificación, cifrado y metadatos

Nivel :B
Alcance: PRO / TEC / PER

Contenidos

- Esquema de clasificación (Público, Uso interno, Restringido, Confidencial).
- Ejemplos prácticos de cada tipo de información en AULASUR.
- Uso del cifrado y cuidado con los metadatos (documentos, imágenes, etc.).

Criterios

- El participante clasifica correctamente casos sencillos de información.
- Sabe cuándo debe cifrar un fichero o correo y cuándo no es necesario.

Roles

- PRO: Responsables de procesos y protección de datos.
- TEC: Personal técnico (configuración de herramientas de cifrado y permisos).
- PER: Personal administrativo, docentes y resto de empleados.

Módulo 3. La información: backups, borrado y tipos de almacenamiento

Nivel: A (especialmente para TEC; contenidos básicos para PER)
Alcance: TEC / PRO / PER

Contenidos

- Concepto de copia de seguridad y regla 3-2-1.
- Diferentes tipos de almacenamiento (local, red, nube) y sus riesgos.
- Borrado seguro de información y pruebas de restauración.

Criterios

- TEC: Conoce y aplica la política de copias de AULASUR y la regla 3-2-1.
- PER: Sabe dónde debe guardar la información de trabajo y qué no debe hacer (no almacenar datos críticos solo en el equipo local).

Roles

- TEC: Personal técnico responsable de sistemas y copias.
- PRO: Dirección / responsables de áreas (entender impacto y recursos necesarios).
- PER: Resto de personal que genera o maneja información.

Módulo 4. El puesto de trabajo: medidas de protección I

Nivel: B
Alcance: PER

Contenidos

- Uso seguro de PCs y portátiles: bloqueo de sesión, no compartir usuario, cuidado físico del equipo.
- Riesgos de memorias USB y otros dispositivos externos.
- Malas prácticas frecuentes en el puesto de trabajo (escenarios H1, H3).

Criterios

- El participante conoce y aplica las normas de bloqueo de equipo y uso de USB.
- Supera el test asociado al recurso del Kit y no ejecuta archivos de USB “trampa” en campañas simuladas.

Roles

- PER: Todo el personal y alumnos que usan equipos de AULASUR.

Módulo 5. El puesto de trabajo: medidas de protección II

Nivel: B
Alcance: PER / PRO

Contenidos

- Limpieza de mesa, gestión de documentos impresos, uso de destructoras.
- Riesgos de shoulder surfing y pantallas visibles a terceros.
- Seguridad física básica en oficinas, aulas y CPD (accesos, llaves, puertas).

Criterios

- El participante reconoce situaciones inseguras (documentos abandonados, pantallas a la vista) y las corrige.
- Se observa una reducción de documentos olvidados en impresoras/zonas comunes.

Roles

- PER: Personal administrativo, docentes, resto de empleados.
- PRO: Dirección y responsables de áreas con gabinetes/archivadores físicos.

Módulo 6. Correo electrónico: principales fraudes y riesgos

Nivel: B
Alcance: PER / PRO

Contenidos

- Tipos de fraudes por correo: phishing, spear-phishing, malware adjunto, estafas económicas.
- Señales de alerta en un correo sospechoso.
- Procedimiento de actuación ante correos dudosos (no clicar, no responder, reportar).

Criterios

- El participante identifica correos fraudulentos en el test del módulo.
- En campañas de phishing simulado (Gophish), disminuye el porcentaje de clics y de envío de credenciales respecto a la primera campaña.

Roles

- PER: Todo el personal y docentes (uso intensivo de correo).
- PRO: Dirección y personal con capacidad de decisión económica (objetivo habitual de fraudes dirigidos).

Módulo 7. Contraseñas y medidas complementarias

Nivel: B
Alcance: PER / TEC

Contenidos

- Requisitos de una contraseña robusta y errores típicos (P2).
- No reutilización ni compartición de credenciales.
- Medidas complementarias: segundo factor de autenticación cuando sea posible, bloqueo automático, etc.

Criterios

- El participante es capaz de distinguir contraseñas fuertes y débiles y de proponer contraseñas adecuadas.
- Supera el test del módulo y acepta las normas internas sobre gestión de contraseñas.

Roles

- PER: Todo el personal y alumnos con acceso al campus o sistemas.
- TEC: Administradores que configuran políticas de contraseñas y MFA.

Módulo 8. Dispositivos móviles y teletrabajo

Nivel: B
Alcance: PER / TEC

Contenidos

- Riesgos específicos de móviles, tablets y portátiles fuera de la oficina (pérdida, robo, redes Wi-Fi abiertas).
- Uso seguro de Wi-Fi corporativa e invitados; obligación de usar VPN en accesos remotos.
- Configuración mínima de seguridad en dispositivos móviles (PIN, cifrado, bloqueo automático).

Criterios

- El participante conoce las normas de uso de Wi-Fi y VPN, y las aplica.
- En encuestas o tests declara seguir prácticas seguras (no acceder a sistemas corporativos desde redes públicas sin VPN, etc.).

Roles

- PER: Personal que teletrabaja o usa dispositivos móviles corporativos/BYOD.
- TEC: Personal técnico encargado de configurar VPNs, Wi-Fi y políticas MDM.

Módulo 9. Redes sociales y presencia digital de la organización

Nivel: B
Alcance: PRO / PER

Contenidos

- Riesgos asociados al uso de redes sociales en el entorno profesional (D4, D5).
- Buenas prácticas para perfiles corporativos de AULASUR y para perfiles personales cuando mencionan a la organización.
- Gestión de incidentes: suplantación de identidad, comentarios ofensivos, filtración de información.

Criterios

- El participante identifica publicaciones inadecuadas en ejemplos prácticos.
- Personas que gestionan perfiles oficiales conocen y aplican el procedimiento ante incidentes en redes sociales.

Roles

- PRO: Dirección, responsables de comunicación/marketing y responsables de área con visibilidad externa.
- PER: Empleados y docentes que puedan referirse a AULASUR en redes sociales.

Evaluación del plan de concienciación

La evaluación del plan de formación y concienciación de AULASUR se realizará basado en la norma ISO 27001, utilizando como base los recursos del Kit de concienciación del INCIBE. El objetivo es comprobar si los usuarios han aprendido y aplican corectamente los contenidos de los módulos y si se produce una reducción real de los riesgos identificados.

Actividades de evaluación

- Tests de conocimientos sobre los módulos del Kit
    - Test al finalizar cada módulo
    - Duración estimada: 10–15 minutos por test.
    - Revisión anual mediante un test .
- Campañas de ataques simulados
    - Phishing (Gophish)
        - Periodicidad: 2 campañas al año (antes y después del ciclo formativo principal).
        - Duración: envíos durante 1 semana y análisis de resultados durante 2 semanas.
    - Memorias USB “infectadas”
        - Periodicidad: 1 vez al año, tras impartir la formación sobre puesto de trabajo.
        - Duración: distribución de USB durante 1 semana y análisis 1 semana.

Indicadores e evidencias

Se utilizarán, como mínimo, los siguientes indicadores:

- Participación y aprovechamiento
    - % de usuarios que completan los módulos que les corresponden (por rol PRO/TEC/PER).
    - % de usuarios que superan los tests con la nota mínima establecida (por ejemplo, ≥ 80 %).
    - Evidencias: registros del campus de formación, listas de asistencia, resultados de tests.
- Resultados de ataques simulados
    - Campañas de phishing:
        - % de clics en enlaces maliciosos.
        - % de introducción de credenciales.
        - % de usuarios que reportan el correo sospechoso.
    - Campañas con USB:
        - Nº de usuarios que conectan el USB y ejecutan el fichero de prueba.
    - Se considerará mejora si estos porcentajes disminuyen respecto a la campaña inicial
- Incidentes y comportamiento real
    - Nº de incidentes ligados a errores humanos (envío de datos al destinatario equivocado, pérdida de dispositivos, documentos abandonados, etc.).
    - Nº de incumplimientos de políticas (desactivar antivirus, instalar software no autorizado, uso indebido de Wi-Fi corporativa).
    - Objetivo: reducción progresiva de este tipo de incidentes.

Evaluación por roles (PRO / TEC / PER)

- PRO (Procesos: dirección y gestión)
    - Evidencias de que conocen sus responsabilidades y toman decisiones considerando la seguridad (actas, aprobación de recursos, revisión de indicadores).
- TEC (Tecnología: personal técnico especializado)
    - Superación de módulos avanzados (backups, DMZ, hardening).
    - Evidencias: procedimientos actualizados, aplicación de la regla 3-2-1, registros de pruebas de restauración, endurecimiento de servicios, etc.
- PER (Personas: todo el personal y alumnos)
    - Superación de módulos básicos (puesto de trabajo, correo, contraseñas, móviles/teletrabajo, redes sociales).
    - Mejora en comportamiento ante campañas simuladas y en el manejo diario de la información.

Periodicidad de revisión del plan

- Recogida y análisis de datos
    - Registros de formación y tests: revisión trimestral.
    - Resultados de campañas de phishing/USB: análisis tras cada campaña.
    - Incidentes relacionados con errores humanos: registro continuo y análisis trimestral.
- Revisiones formales
    - Revisión intermedia: cada 6 meses, reunión de aproximadamente 1 hora.
    - Revisión anual completa del plan: 1 vez al año, reunión de unas 2 horas para analizar todos los indicadores y proponer mejoras.

El plan de concienciación se actualizará al menos una vez al año en función de los resultados obtenidos, de los incidentes ocurridos y de los cambios en el contexto.

Apartado 4: Detallar los materiales de formación y concienciación utilizados.

Para los materiales de formación nos basaremos en los ofrecidos por el Kit de concienciación del INCIBE adaptados a AULASUR.

Categoría de Material	Descripción
Poster/Cartel	Imágenes diseñadas para ser impresas y ubicadas en lugares visibles. Envía mensajes claros breves y precisos con lenguaje claro. También pueden ser informativos como las normas del aula.
Presentación	Archivos PowerPoint (o similar) con resúmenes y conceptos que un tutor irá desarrollando en un curso online o presencial. Posteriormente podrá ser subido a una plataforma online para su descarga o enviado por email
Documento PDF	Desarrollo detallado de los conceptos y los módulos.
Email	Imágenes con mensajes cortos para ser distribuidas por correo electrónico corporativo o intranet. También se podrá insertar al pie de cada correo como firma con mensaje recordatorio de buenas prácticas
Newsletter	Publicación periódica para divulgar novedades y reforzar mensajes, que puede ser interna o externa.
Curso / Formación	Programa formativo completo y sesiones (a menudo basado en la Presentación y el PDF) que debe realizarse periódicamente.
Test de evaluación	Pruebas tipo test para calificar el conocimiento asimilado tras la formación.
Encuesta de satisfacción	Encuesta realizada por los usuarios para comprobar el nivel de satisfacción tras recibir la formación

Algunos ejemplos

Póster: Normas del aula de informática

- Objetivo: Recordatorio de buenas prácticas en el uso de equipos en las aulas.
- Formato A3.
- Ubicación: aulas.

Cartel: "Bloquea tu equipo antes de levantarte"

Objetivo: Evitar accesos no autorizados a equipos desatendidos (escenarios H3, I3).

Formato y ubicación:

- Formato A3 y versión digital para salvapantallas.
- Ubicación: aulas, oficinas, recepción y zonas de trabajo compartidas.

Contenido del cartel (texto):

Consejos de buenas prácticas de bloquear el ordenador al abandonar el puesto

Presentación multimedia:

Objetivo: Sirve de apoyo a tutor que imparte curso basico de ciberseguridad. Puede ir dirigido a alumnos o nuevos trabajadores como curso de bienvenida**.**

Formato y ubicación:

- Formato PDF o PowerPoint.
- Ubicación: En ordenador de tutor de curso o subido a la plataforma para descarga por parte de alumnos que reciben la formación.
- Ver ejemplo en Powerpoint

Encuesta de satisfacción: (También tenemos la encuesta que aporta el INCIBE en el kit de concienciación)

- Tipo de material: Encuesta online.
- Destinatarios: Todo el personal que reciba la formación
- Canal: Enlace enviado por correo tras la sesión o enlazado desde la última diapositiva.
- Contenido detallado: Ver encuesta
- Esta encuesta sirve para medir la satisfacción y utilidad percibida y recoger ideas para mejorar el plan de concienciación en próximas ediciones.

Apartado 5: Detallar las Auditorías Internas de cumplimiento en prevención.

Las auditorías internas de prevención tienen como objetivo **verificar que los materiales de formación y concienciación definidos en los apartados anteriores se están utilizando realmente**, para ello se utilizarán formularios tipo checklist, donde se irán registrando los que cumplen los requisitos y los que no.

Las auditorías comprobarán:

- Que los materiales existen, están actualizados y se han difundido por el canal previsto.
- Que han llegado a los roles definidos (PRO/TEC/PER)**.**
- Que se han obtenido evidencias de su uso y eficacia (tests, métricas de campañas, etc.).

Hardware (H1–H4)

Escenario H1: Malware por USB / dispositivos externos

- **Correo electrónico**
  - Envío de recordatorios periódicos con el mensaje “Piensa antes de enchufar” y enlace al recurso del Kit sobre puesto de trabajo.
  - **En auditoría**: revisar histórico de campañas de correo, destinatarios, frecuencia (al menos 1 vez/año) y tasa de apertura.
- **Intranet corporativa**
  - Publicación fija de una ficha “Uso seguro de dispositivos USB” dentro del portal de seguridad.
  - **En auditoría**: comprobar existencia, fecha de actualización y estadísticas de acceso.
- **Vídeos en salas comunes / campus**
  - Vídeo corto del Kit sobre puesto de trabajo, proyectado en aulas y disponible en el campus.
  - **En auditoría**: verificar calendario de reproducción y evidencia de que se ha incluido en las acciones formativas.
- **Carteles y trípticos**
  - Cartel “Piensa antes de enchufar (USB)” en aulas de informática y zona de profesores.
  - **En auditoría**: recorrido físico y checklist de presencia/estado de la cartelería.
- **Otros (ataques simulados)**
  - **Campaña anual** de memorias USB “infectadas” del Kit.
  - **En auditoría**: informe con nº de USB repartidos, nº de ejecuciones y conclusiones.

Escenarios H2–H3: Portátiles sin proteger y equipos sin bloquear

- **Correo electrónico**: recordatorio semestral sobre bloqueo de sesión y protección física de portátiles.
- **Intranet**: guía PDF “Buenas prácticas con portátiles” accesible en el portal.
- **Carteles**: banda estrecha “ANTES DE LEVANTARTE… BLOQUEA TU EQUIPO” sobre cada monitor.

- **Vídeos**: inclusión de un bloque específico sobre portátiles/bloqueo en los vídeos de bienvenida a empleados.

Auditoría:

- Muestreo de puestos para verificar presencia de carteles.
- Revisión de envíos de correo e inclusión del tema en las sesiones grabadas.
- Entrevistas/cuestiones rápidas a usuarios (muestra) sobre el atajo Win+L.

Escenario H4: Acceso indebido a servidores e inventario de activos

- **Intranet**: documentación técnica y procedimiento de acceso seguro al inventario de activos.
- **Correo**: comunicación dirigida a personal técnico cuando se actualizan normas o procedimientos.
- **Otros**: sesión técnica basada en el ejercicio "Ataque a un inventario de activos" (presencial u online).

Auditoría:

- Revisión de la documentación en intranet (vigencia, control de versiones).
- Comprobación de convocatorias y asistentes a la sesión técnica.

Sofware

Escenarios S1–S2: Actualizaciones y uso de antivirus / EDR

- **Correo electrónico**: avisos planificados de ventanas de actualización y recordatorio de no desactivar antivirus.
- **Intranet**: sección "Estado de seguridad" con información sobre parches críticos y política de antivirus.
- **Carteles**: mensajes breves tipo "No desactives tu antivirus" en zonas técnicas.

Auditoría:

- Muestreo de comunicaciones publicadas y evidencias de que se informan los cambios.
- Verificación de que la sección de intranet está actualizada.

Escenario S3: Phishing y adjuntos maliciosos

- **Correo electrónico**: envío de boletines de concienciación y correos simulados de phishing (Gophish).
- **Intranet**: módulo de e-learning sobre "Fraudes por correo", con test final.
- **Vídeos**: vídeo explicativo sobre phishing incluido en las sesiones generales.
- **Carteles**: póster "Piensa antes de hacer clic".

Auditoría:

- Informes de campañas de phishing (tasa de clics, reportes) y evidencias de progreso.
- Registros de realización y superación del módulo online.
- Verificación física de la cartelería.

Escenario S4: Software no autorizado / sin licencia

- **Correo electrónico**: recordatorios sobre la política de software y consecuencias.
- **Intranet**: lista de software aprobado y procedimiento de solicitud de nuevas herramientas.
- **Otros**: controles técnicos de inventario de software.

Auditoría:

- Revisión de comunicaciones y de la política en intranet.
- Muestreo de equipos para detectar software no autorizado.

Comunicaciones

Escenarios C1: Servicios expuestos en DMZ

- **Intranet**: documentación para técnicos sobre diseño de DMZ y checklist de revisión.
- **Otros**: sesiones técnicas periódicas.

Auditoría:

- Revisión de checklists cumplimentados y evidencias de revisión de servicios expuestos.

Escenario C2: Navegación insegura

- **Correo electrónico**: campañas de “Navegación segura en la empresa”.
- **Intranet**: consejos prácticos y FAQ.
- **Carteles**: mensajes en zonas comunes sobre webs de riesgo.

Auditoría:

- Evidencias de envíos y publicaciones, y análisis de logs web (por IT) para ver descenso de tráfico a categorías bloqueadas.

Escenarios C3–C4: Wi-Fi corporativa y teletrabajo sin VPN

- **Correo**: instrucciones de uso de Wi-Fi y VPN a personal que teletrabaja o usa portátiles.
- **Intranet**: guía paso a paso de VPN.
- **Vídeos**: breve clip sobre riesgos en Wi-Fi públicas.

Auditoría:

- Muestreo de equipos para comprobar configuración correcta de VPN.
- Revisión de estadísticas de conexiones por VPN.

Instalaciones

Escenarios: I1–I3

- **Correo**: recordatorios sobre limpieza de mesa y recogida de impresiones.
- **Carteles y trípticos**: carteles de "Limpieza de mesa" junto a impresoras y en zonas de archivo.
- **Vídeos**: inclusión de seguridad física básica en vídeos de bienvenida.

Auditoría:

- Recorridos físicos y checklist de cumplimiento (documentos abandonados, puertas cerradas, etc.).
- Evidencia de que se incluyen estos contenidos en la formación inicial.

Datos

Escenarios: D1–D5

- **Correo**: avisos sobre protección de datos, uso de CCO, cifrado de adjuntos.
- **Intranet**: esquema de clasificación de la información y guías de protección de datos.
- **Carteles**: "Cuida tus datos, cuida AULASUR" en áreas administrativas.
- **Otros**: ejercicios prácticos y revisión de casos reales en sesiones formativas.

Auditoría:

- Comprobación de que las guías están publicadas y divulgadas.
- Muestreo de correos enviados (cumplimiento de CCO, no uso de datos excesivos).
- Revisión de incidentes de protección de datos.

Personas y redes sociales

Escenarios:P1–P2, D4–D5

- **Correo**: campañas de concienciación sobre contraseñas y redes sociales.
- **Intranet**: política de uso de redes sociales y normas sobre imagen corporativa.
- **Vídeos**: pequeñas cápsulas de vídeo sobre ingeniería social y reputación online.
- **Carteles**: "Tu contraseña es la llave", "Lo que subes a redes no se borra".

Auditoría:

- Revisión de que todo el personal ha recibido los mensajes clave (listados de distribución).
- Comprobación de que la política de redes sociales está publicada y aceptada (firmas o clic de aceptación).
- Revisión periódica de perfiles oficiales y menciones a AULASUR en redes (muestreo).

Otros medios de apoyo

Además de los canales anteriores, las auditorías internas revisarían:

- **Sesiones presenciales/online** (asistencia, contenidos, actas).
- **Cuestionarios de evaluación y encuestas de satisfacción** (resultados y mejoras propuestas).
- **Documentación de soporte** (procedimientos, normas, guías) como evidencia de que la formación y concienciación están integradas en el sistema de gestión.

Material a usar en la auditoría e indicadores de logro

Ataques simulados de malware (USB, ficheros maliciosos)

Material a revisar en la auditoría

- Plantillas de ficheros del **ejercicio de memorias USB infectadas** del Kit del INCIBE.
- Registro de **usuarios y áreas en las que se han dejado los USB**.
- **Informe de resultados** de la campaña: nº de USB recogidos, nº conectados, nº de ejecuciones del fichero, mensajes mostrados, etc.
- Evidencias de **acciones de refuerzo** tras la campaña (correos explicativos, sesiones breves, actualización de carteles).

Indicadores de logro (Apto / No apto)

- **A nivel individual (usuario):**
    - **Apto:** no conecta el USB desconocido **o**, si lo conecta, no ejecuta el fichero y lo entrega a Soporte / lo reporta.
    - **No apto:** conecta el USB y ejecuta el fichero “trampa” sin consultar.
- **A nivel global (organización/grupo):**
    - Se considera **Apto** si:
        - Menos del **20 %** de los usuarios que encontraron un USB ejecutan el fichero en la primera campaña.
        - Y en campañas posteriores se observa una **tendencia descendente** (por ejemplo, reducción ≥ 30 % respecto a la línea base).
    - **No apto** si el porcentaje de ejecución es alto (≥ 20–25 %) o no mejora en campañas sucesivas.

En caso de **No apto**, se deberán planificar **acciones de formación adicional** insistiendo sobre el uso de dispositivos externos y reforzar cartelería y correos de concienciación.

Campañas de simulación de phishing

Material a revisar en la auditoría

- Plantillas de correos usados en la campaña (diseñados con Gophis).
- Registro de **destinatarios y grupos** objetivo (por rol: PRO/TEC/PER).
- **Informe de resultados de la campaña**:
  - nº de correos enviados y entregados.
  - nº y % de usuarios que hacen clic en el enlace.
  - nº y % de usuarios que introducen credenciales.
  - nº y % de usuarios que reportan correctamente el correo como sospechoso.
- Evidencias de **feedback posterior** (correo explicativo, mini-sesiones, actualización de módulos formativos).

Indicadores de logro (Apto / No apto)

- **A nivel individual (usuario):**
  - **Apto:** no hace clic en el enlace **o**, si hace clic, no introduce credenciales y reporta el correo como sospechoso.
  - **No apto:** introduce credenciales en el formulario falso, o bien hace clic repetidamente en varias campañas.
- **A nivel global (organización/grupo):**
  - Primera campaña (línea base): se toma solo como referencia.
  - En campañas posteriores se considerará **Apto** el grupo/organización si:
    - % de clics en el enlace es **< 15 %**.
    - % de usuarios que introducen credenciales es **< 5 %**.
    - % de usuarios que reportan correctamente el correo es **≥ 30 %** y va aumentando campaña a campaña.
  - Se considerará **No apto** si:
    - Los porcentajes de clics y/o de credenciales son altos (≥ 20 % y ≥ 5–10 % respectivamente),
    - O no hay mejora significativa respecto a la campaña anterior.

En caso de **No apto**, se reforzarán los módulos de **correo electrónico y phishing**, se repetirán campañas concretas para los grupos con peor resultado y se revisarán mensajes y materiales para hacerlos más claros y visibles.