Presentación general

- **Propósito:** desarrollar hábitos diarios que protejan la información de PRODAC.
- **Ejes:** Confidencialidad, Integridad y Disponibilidad (CIA), responsabilidad compartida, respuesta ante incidentes.
- **Formato:** 7 módulos progresivos con teoría breve, tarjetas interactivas, casos prácticos y checklist; examen final con banco de 30 preguntas (se muestran 15 al azar).
- **Perfil del participante:** todo colaborador (administrativo, operativo, mando medio, jefatura).
- **Resultados de aprendizaje:**
    - Identificar amenazas comunes y señales de fraude.
    - Usar de forma segura cuentas, correo, Internet y dispositivos.
    - Proteger datos personales/corporativos y respetar políticas internas.
    - Actuar correctamente ante incidentes y reportar por canales oficiales.

Módulo 1. Introducción a la Ciberseguridad y Responsables

Qué verás

- ¿Por qué cuidamos la información? La triada CIA:
    - **Confidencialidad:** acceso solo para autorizados.
    - **Integridad:** datos completos y sin alteraciones.
    - **Disponibilidad:** sistemas e información cuando se necesitan.
- Responsabilidad compartida:
    - **Gerencia de TI:** estrategia, políticas, activación de protocolos.
    - **Soporte/Infraestructura:** monitoreo, contención, recuperación, comunicación técnica.
    - **Colaboradores:** uso responsable, criterio ante dudas, reporte inmediato.
- Políticas internas clave (uso de recursos, credenciales, software, datos).

Caso práctico – *"El archivo modificado"*
Detectas cifras alteradas en un reporte financiero oficial → se compromete la **integridad**.

Actividades

- Tarjetas de conceptos CIA.
- Mini-quiz de reconocimiento del principio afectado.

Checklist

- Sé a quién reportar.
- Sé que mis decisiones diarias también son seguridad.
- Identifico CIA en ejemplos cotidianos.

Módulo 2. Tu cuenta, tus contraseñas y 2FA

Qué verás

- Identidad digital (tu usuario = tu DNI; tu contraseña = tu llave).
- Contraseñas seguras: longitud (≥8), **frases robustas**, entropía, gestores aprobados, no reutilización.
- 2FA/MFA: qué es, por qué bloquea accesos aun si roban la contraseña, códigos de respaldo.
- Errores comunes vs buenas prácticas (post-its, contraseñas repetidas, ignorar 2FA).

Caso práctico – *"El descuido de Ana"*
Correo de *soporte@pr0dac.com* (cero por "o"), enlace falso, misma clave en redes y trabajo, 2FA desactivado → múltiples riesgos y cómo evitarlos.

Actividades

- Tarjetas comparativas "error / buena práctica".
- Mini-quiz: detectar homógrafos y decisiones seguras.

Checklist

- Mis contraseñas son únicas y robustas.
- 2FA activo en cuentas críticas.
- Verifico dominios antes de ingresar credenciales.

Módulo 3. Correo e Internet sin trampas

Qué verás

- Uso correcto del correo corporativo: adjuntos ligeros, **enlaces compartidos** (OneDrive/SharePoint), nunca enviar contraseñas.
- Navegación segura: sitios permitidos, extensiones/permisos, descargas solo de fuentes oficiales.
- Phishing: señales (urgencia, remitente raro, adjuntos inesperados, **URL parecidas**).
- **Qué es una URL** (explicado simple): la "dirección" del sitio (ej. https://www.google.com). Cambiar una letra (ej. go0gle) ya es otro lugar.
- Archivos con macros: "Habilitar contenido" y riesgos.

Caso práctico – *"Factura urgente"*
Llega FACTURA_URGENTE.xlsm solicitando habilitar macros → no habilitar, confirmar por teléfono, consultar a TI.

Actividades

- Tarjetas de "señales de phishing".
- Mini-quiz de macros y verificación de enlaces.

Checklist

- Solo uso el correo para trabajo.
- No habilito macros inesperadas.
- Verifico remitente y URL exacta antes de hacer clic.

Módulo 4. Archivos, Excel, USB y tu equipo

Qué verás

- USB y discos externos: política corporativa, **baiting** (anzuelo), riesgos de malware.
- Guardado/compartido: carpetas corporativas y OneDrive/SharePoint; evitar datos sensibles en el Escritorio; permisos correctos; clasificación de información.

- Tu equipo: no instalar software no autorizado, no cambiar red; bloqueo **Win+L**; actualizaciones y antimalware.

Caso práctico – *"USB anzuelo"*
Encuentras un USB "Planillas" → no conectarlo; entregar a TI.

Actividades

- Tarjetas de "dónde guardar" y "cómo compartir".
- Mini-quiz: decisiones correctas con USB y Excel.

Checklist

- Evito conectar USB desconocidos.
- Comparto con enlaces y permisos.
- Bloqueo mi equipo al levantarme.

Módulo 5. Amenazas digitales y fraudes más comunes (mega-módulo)

Qué verás *(explicado sin tecnicismos, con ejemplos de oficina)*

- **Malware**: virus, gusanos, troyanos (se disfrazan), **spyware/keyloggers** (espían), **adware**, **backdoors**.
- **Ransomware**: cómo entra (correo/enlace/USB), en qué consiste (cifrado + nota de rescate), qué NO hacer (pagar), cómo se contiene (aislar, avisar, respaldos).
- **Ingeniería social**: phishing (correo/páginas), **smishing** (SMS), **vishing** (llamadas), **QRishing** (QR falsos), **BEC** (suplantación de jefe/proveedor).
- **Riesgos web**: malvertising, descargas de "navegadores" falsos, extensiones invasivas, sitios HTTP, cookies y rastreadores.
- **Buenas prácticas que cortan la mayoría del riesgo**:
    - No abrir lo que no esperas.
    - Confirmar por teléfono lo sensible.
    - Mantener el equipo actualizado y con 2FA.
    - Principio de mínimo privilegio.

Casos prácticos

1. *"Orden de pago urgente"* (BEC): correo del "jefe" pidiendo transferir a nueva cuenta → verificar canal formal y flujos de aprobación.

2. *“Descarga de navegador”* (malvertising): banner que ofrece “Chrome rápido” → descargar solo desde sitio oficial.
3. *“QR del estacionamiento”* (QRishing): cartel con QR a “pago” → validar con administración y no ingresar credenciales.

Actividades

- Tarjetas interactivas por tipo de amenaza.
- Mini-quizzes temáticos.

Checklist

- Dudo de urgencias y cambios de último minuto.
- Descargo solo desde fuentes oficiales.
- Reporto intentos de fraude al canal oficial.

Módulo 6. Protección de datos y privacidad digital

Qué verás

- Tipos de datos: **personales**, sensibles, confidenciales, uso interno, públicos.
- Principio de **mínimo privilegio** y “necesidad de saber”.
- **Cifrado**: en tránsito (https/TLS) y en reposo (archivos cifrados), envío seguro de documentos, nunca contraseñas por correo.
- **Cookies y privacidad**: “solo necesarias” en trabajo; configuración básica si un sitio no carga; evitar trackers innecesarios.
- Exposición en redes sociales, fotos con **metadatos** (EXIF), compartir planillas con datos reales.
- Envío a terceros y retención de datos: autorizaciones, acuerdos, tiempo de conservación.

Caso práctico – *“Planilla pública sin querer”*
Planilla de clientes compartida por enlace “público con cualquiera” → cómo revocar, notificar y prevenir.

Actividades

- Tarjetas de clasificación de datos.
- Mini-quiz de privacidad y cifrado.

Checklist

- Clasifico datos antes de compartir.
- Uso cifrado cuando corresponde.
- Reviso permisos de acceso y duración.

Módulo 7. Cuando algo pasa: actuación y qué hace PRODAC

Qué verás

- Qué es un incidente (sospecha/confirmado): ejemplos prácticos.
- **Guion en 5 pasos**:
    1. No abrir/clic/insertar.
    2. Preservar evidencia (capturas/horas), **no reenviar** archivos sospechosos.
    3. Avisar de inmediato a jefe y TI por canal oficial.
    4. Si hay comportamiento extraño/cifrado, aislar de la red.
    5. Esperar instrucciones (contención, análisis, restauración).
- Qué hace PRODAC: respaldos, monitoreo, mantenimiento, contingencias (sitios alternos, UPS/grupo electrógeno).
- **Ficha dorada de contacto** (tarjeta "revelable"):
    - **Canal oficial:** *correo de seguridad*, *Helpdesk*, *extensión interna* (reemplazar por datos reales).
    - **Qué enviar:** descripción breve, cuándo empezó, capturas (sin reenviar malware), equipo afectado, datos de contacto.

Caso práctico – *"Instalé un software no autorizado"*
Cómo actuar, qué reportar, por qué importa para la contención y trazabilidad.

Actividades

- Simulación de reporte inicial.
- Mini-quiz de preservación de evidencia.

Checklist

- Sé cómo reportar y por dónde.
- Conozco el guion de 5 pasos.

- Entiendo que incumplir políticas tiene consecuencias.

Evaluación final (bloqueada hasta completar el Módulo 7)

- **Banco de 30 preguntas** (escenarios laborales reales); el sistema **muestra 15 aleatorias** por intento.
- Retroalimentación inmediata por pregunta.
- Criterio de aprobación recomendado: **≥80%**.
- Reintento habilitable según política interna.
- Evidencia de cumplimiento (fecha, puntaje, módulos completados).

Requisitos y metodología

- **Requisitos técnicos:** navegador actualizado, audio opcional, conexión estable; acceso a correo corporativo/OneDrive.
- **Metodología:** micro-lecciones con tarjetas, casos prácticos, checklists operativos, retroalimentación inmediata.
- **Duración sugerida:** 7 módulos × 30–40 min + evaluación 20–25 min (total 4.5–5.5 h).
- **Accesibilidad:** lenguaje claro, ejemplos cotidianos, tipografías legibles, contraste adecuado.

Métricas de eficacia (sugeridas)

- Tasa de **reporte temprano** de phishing/incidentes.
- Reducción de **clics** en simulaciones de phishing.
- Cumplimiento de **2FA** y complejidad de contraseñas.
- Correcciones de **permisos** en documentos compartidos.

Anexos

- **Glosario básico:** CIA, 2FA, phishing/smishing/vishing, ransomware, homógrafos, QRishing, mínimo privilegio, cifrado, metadatos EXIF.
- **Plantillas:**

- Formato de **reporte de incidente** (qué/cuándo/cómo/evidencia/contacto).
- Guía rápida de **verificación de URL**.
- Guía para **compartir con OneDrive/SharePoint** (permisos recomendados).