Curso de Ciberseguridad PRODAC

Autor: Área de Tecnología de la Información

Afiliación: PRODAC

Programa: Capacitación Corporativa

Fecha: 2025

Resumen

Este curso introduce, en lenguaje sencillo, los hábitos y decisiones diarias que mantienen segura la información de PRODAC. Combina reglas internas con prácticas de concienciación: manejo de cuentas y contraseñas, uso de correo e Internet, trabajo con archivos y Excel, dispositivos USB, llamadas y mensajería, identificación de amenazas (virus, troyanos, ransomware, phishing, vishing, smishing), cuidado de cámara web, diferencias entre HTTP y HTTPS, cookies y actuación ante incidentes. Está diseñado para personas sin conocimientos técnicos, con casos prácticos, listas de verificación y una evaluación final de 25 preguntas.
Palabras clave: ciberseguridad, contraseñas, phishing, ransomware, USB, Excel, 2FA, http/https, cookies, vishing, smishing

Índice del Curso de Ciberseguridad PRODAC

Módulo 1. Introducción y responsabilidades

1.1 ¿Por qué cuidamos la información?
1.2 Quién hace qué en PRODAC
1.3 Seguridad física visible
1.4 Caso práctico y lista de verificación

Módulo 2. Tu cuenta, tus contraseñas y 2FA

2.1 Reglas simples que sí debes saber
2.2 Buenos hábitos diarios
2.3 Altas, cambios y bajas
2.4 Caso práctico y lista de verificación

Módulo 3. Correo e Internet sin trampas

3.1 Correo (uso laboral, adjuntos y enlaces)
3.2 Internet (navegación filtrada)
3.3 Phishing (cómo huele y cómo evitarlo)
3.4 Excel y la barra "Habilitar contenido"
3.5 Caso práctico y lista de verificación

Módulo 4. Archivos, Excel, USB y tu equipo

4.1 USB y discos externos
4.2 Guardado y compartido de archivos
4.3 Tu equipo (software y bloqueo)
4.4 Caso práctico y lista de verificación

Módulo 5. Amenazas frecuentes (explicadas para usuarios)

5.1 Malware en simple: virus, troyanos, spyware y keyloggers
5.2 Ransomware
5.3 Phishing y familia: smishing, vishing y spoofing
5.4 Web confiable: HTTP vs. HTTPS, dominio exacto y cookies
5.5 Cámara web y permisos
5.6 Hábitos que reducen la mayoría del riesgo

Módulo 6. Llamadas, WhatsApp y mensajería

6.1 Teléfono corporativo
6.2 Engaños por llamada o mensaje
6.3 Guion de respuesta de 3 pasos

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

7.1 Guion en 5 pasos ante sospecha o incidente
7.2 Lo que PRODAC ya tiene
7.3 Sanciones (en simple)
7.4 Casos cortos y lista de verificación

Evaluación final (25 preguntas)

A. Conocimiento aplicado (15 preguntas)
B. Situaciones del día a día (10 preguntas)

Módulo 1. Introducción y responsabilidades

1.1 ¿Por qué cuidamos la información?

Cuidamos la confidencialidad, integridad y disponibilidad de los datos de PRODAC. La ciberseguridad es parte del trabajo diario: hábitos sencillos evitan la mayoría de incidentes.

1.2 Quién hace qué en PRODAC

Gerencia de TI: coordina la seguridad y activa medidas ante incidentes.

Soporte e Infraestructura: identifica riesgos, ayuda a recuperar servicios y comunica pautas.

Cada colaborador: usa bien los recursos, duda con criterio y reporta de inmediato lo sospechoso.

1.3 Seguridad física visible

Las salas técnicas poseen control de acceso (por ejemplo, biometría o código), detección de humo y señalización de acceso restringido. Sin autorización, no se ingresa.

1.4 Caso práctico y lista de verificación

Caso: Un visitante solicita ver “rápido” el área de servidores. Decisión correcta: no permitir el acceso sin autorización formal; escalar a tu jefe y TI.

Checklist:

• ¿Sé a quién avisar si algo me parece sospechoso (jefe y TI)?

• ¿Entiendo que mis decisiones diarias también son seguridad?

Módulo 2. Tu cuenta, tus contraseñas y 2FA

2.1 Reglas simples que sí debes saber

El usuario es personal e intransferible. Las contraseñas deben tener, como mínimo, 6 caracteres combinando letras, números y símbolos. Hay cambios periódicos e intentos fallidos limitados que bloquean la cuenta por seguridad. Se usa doble factor de autenticación (2FA).

2.2 Buenos hábitos diarios

No reutilices la misma clave en trabajo y en redes personales. No compartas tu contraseña ni los códigos 2FA. Considera un gestor de contraseñas aprobado por TI.

2.3 Altas, cambios y bajas

Los accesos se solicitan por correo con participación del jefe y las áreas responsables; TI configura lo aprobado. Al cese, TI da de baja la cuenta en un plazo breve; puede redirigir temporalmente el correo y respaldar información si corresponde.

2.4 Caso práctico y lista de verificación

Caso: Mensaje para “actualizar contraseña” con enlace que parece correcto pero usa caracteres alterados (por ejemplo, pr0dac con cero). Decisión correcta: no entrar; reportar a TI y eliminar.

Checklist:

• ¿Mi contraseña es solo mía y distinta a mis redes?

• ¿Tengo activo el 2FA?

• ¿Verifiqué que el dominio sea el oficial antes de ingresar?

Módulo 3. Correo e Internet sin trampas

3.1 Correo (uso laboral, adjuntos y enlaces)

El correo es para fines laborales. Los adjuntos ligeros pueden enviarse por correo; si pesan mucho, usa OneDrive o SharePoint y comparte enlace con permisos adecuados. Evita enviar contraseñas por correo o dentro de archivos.

3.2 Internet (navegación filtrada)

La navegación está filtrada: se permiten sitios necesarios para trabajar; accesos especiales se solicitan por correo al jefe. No cambies configuraciones ni instales navegadores no autorizados.

3.3 Phishing (cómo huele y cómo evitarlo)

Señales: urgencia, faltas, remitente genérico, logotipos dudosos, enlaces con dominios parecidos al real y adjuntos inesperados. Variantes: smishing (SMS) y vishing (llamadas).

3.4 Excel y la barra “Habilitar contenido”

Si no esperabas el archivo, no habilites macros. Confirma por teléfono con el remitente y consulta a TI.

3.5 Caso práctico y lista de verificación

Caso: Llega ‘FACTURA_URGENTE.xlsm’ y Excel pide “Habilitar contenido”. Decisión: no habilitar; confirmar por teléfono y consultar a TI.

Checklist:

• ¿Esperaba ese correo y ese adjunto?

• ¿El enlace es exactamente el dominio oficial (https y nombre correcto)?

• ¿Para archivos pesados utilicé OneDrive o SharePoint?

Módulo 4. Archivos, Excel, USB y tu equipo

4.1 USB y discos externos

Evita conectar USB personales o desconocidos; suelen estar deshabilitados por seguridad, salvo autorización. Un USB ‘olvidado’ puede ser un anzuelo (baiting).

4.2 Guardado y compartido de archivos

Usa carpetas corporativas y OneDrive o SharePoint; evita dejar bases sensibles en el Escritorio. No pongas contraseñas dentro de Excel ni al pie del correo.

4.3 Tu equipo (software y bloqueo)

No instales ni desinstales programas por tu cuenta. No cambies ajustes de red. Bloquea tu PC al moverte con Windows + L; además, el equipo se bloquea solo tras inactividad.

4.4 Caso práctico y lista de verificación

Caso: Encuentras un USB rotulado “Planillas” en una sala. Decisión: no conectarlo; entregarlo a TI.

Checklist:

• ¿Evito conectar USB personales o desconocidos?

• ¿Comparto archivos pesados con enlace y permisos adecuados?

• ¿Bloqueo mi PC cuando me levanto (Win + L)?

Módulo 5. Amenazas frecuentes

5.1 Malware en simple: virus, troyanos, spyware y keyloggers

Virus: se propaga e infecta archivos o sistemas. Troyano: se disfraza de algo útil para entrar y abrir puertas a atacantes. Spyware/Keylogger: espían la actividad o registran teclas, pudiendo robar credenciales.

5.2 Ransomware

Secuestra archivos mediante cifrado y exige pago. Variantes: scareware, cryptolocker y bloqueo de pantalla. Prevención: no abrir adjuntos dudosos, mantener el equipo actualizado, usar antivirus y confiar en copias de seguridad. Ante sospecha: no pagar; avisar a TI y seguir el guion de incidentes.

5.3 Phishing y familia: smishing, vishing y spoofing

Phishing: correos/páginas falsas que imitan sitios reales para robar datos. Smishing: engaños por SMS. Vishing: llamadas que fingen ser del banco/soporte pidiendo claves o códigos. Spoofing: dominios o nombres casi iguales a los reales.

5.4 Web confiable: HTTP vs. HTTPS, dominio exacto y cookies

HTTP (sin candado): no ingreses credenciales sensibles en sitios externos. HTTPS (con candado): cifra la conexión, pero aún debes verificar el dominio. Es preferible escribir el nombre oficial o usar marcadores corporativos; cuidado con caracteres raros. Sobre cookies: en trabajo, prioriza “solo necesarias” o configura lo mínimo para que funcione.

5.5 Cámara web y permisos

No otorgues permisos de cámara o micrófono a sitios o extensiones desconocidos. Usa plataformas oficiales y revisa permisos del navegador. Si no usas la cámara, puedes taparla físicamente.

5.6 Hábitos que reducen la mayoría del riesgo

No abras lo que no esperas; confirma por teléfono cuando dudes. Mantén tu equipo actualizado y consulta a TI ante comportamientos extraños.

Módulo 6. Llamadas, WhatsApp y mensajería

6.1 Teléfono corporativo

El uso es laboral y con autorización; la clave telefónica es personal.

6.2 Engaños por llamada o mensaje

Vishing: nadie debe pedirte contraseñas o códigos por teléfono. Smishing: enlaces en SMS que buscan datos o descargas. Si algo suena ‘demasiado bueno’ o ‘muy urgente’, desconfía.

6.3 Guion de respuesta de 3 pasos

1) No compartas datos ni sigas enlaces.

2) Corta y/o deniega la solicitud.

3) Reporta a TI por canal oficial.

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

7.1 Guion en 5 pasos ante sospecha o incidente

1) No abrir/clic/insertar.

2) Captura evidencia (pantalla/fecha), sin reenviar archivos.

3) Avisa a tu jefe y a TI de inmediato.

4) Si la PC se comporta raro (alertas/cifrado), desconéctate de la red.

5) Espera instrucciones de TI (contención, restauración, etc.).

7.2 Lo que PRODAC ya tiene

Backups y procedimientos de restauración; monitoreos periódicos de carpetas, Internet, red interna y equipos; mantenimiento de equipos; contingencias con sitios alternos y sistemas de energía (por ejemplo, UPS).

7.3 Sanciones (en simple)

Instalar software no autorizado, navegar donde no corresponde, mal uso de equipos o pérdida por descuido puede acarrear amonestación, suspensión o despido, según el caso y recurrencia.

7.4 Casos cortos y lista de verificación

“Instalé un conversor PDF por mi cuenta”: pide a TI herramientas aprobadas.

“El banco me pide mi código 2FA”: cuelga y reporta. Nadie debe pedirte códigos.

Checklist:

• ¿Sé qué no debo hacer ante sospecha?

• ¿Sé que la empresa ya tiene copias y planes?

• ¿Sé que romper reglas tiene consecuencias?

Evaluación final (25 preguntas)

Referencias

PRODAC. (s. f.). P-SIG-SIS-002: Seguridad de la Información y del Sistema Informático. Documento interno de PRODAC.

PRODAC. (s. f.). Infografías de concienciación en ciberseguridad. Material interno de PRODAC.