

Caso práctico de phishing para FP

Ficha del alumnado. Analiza un incidente ficticio, propone una primera respuesta y documenta decisiones. El objetivo es justificar cada paso con evidencias y distinguir hechos de cuestiones pendientes.

Equipo _____ Grupo _____ Fecha _____

60 minutos en equipos de tres. Lectura 10 min; prioridades 15 min; registro y aviso 20 min; contraste y evaluación 15 min.

Simulación de aula sobre el papel o en este documento. No envíes mensajes, abras enlaces ni uses credenciales reales. Todas las direcciones, horas y entidades son ficticias.

El caso de Suministros Norte

Suministros Norte es una distribuidora ficticia. Su equipo usa el correo para pedidos y comunicaciones con proveedores. A las 09:02, una persona de administración recibe un mensaje que afirma que su buzón se bloqueará si no renueva el acceso. El procedimiento interno establece que los problemas de cuenta se comunican a informática por el canal de soporte habitual.

Remitente mostrado: Soporte de Suministros Norte. Dirección: soporte@norte-suministros.invalid. Asunto: Renueva tu acceso antes de las 10:00. Texto: Para evitar el bloqueo del buzón, confirma hoy tu usuario y contraseña. Enlace desactivado: hxxps://acceso.norte-suministros.invalid/verificar.

Referencia	Hecho conocido
E1 · 09:02	Llega el mensaje que pide renovar las credenciales.
E2 · 09:04	La persona declara que abrió el enlace e introdujo las credenciales de su correo.
E3 · 09:06	La persona informa por el canal interno de soporte. Conserva el mensaje y declara que no descargó ningún archivo.
E4 · 09:10	Informática confirma por el canal interno que no solicitó esa renovación.

No se han revisado registros de acceso. Lectura de mensajes, cambios de configuración y extracción de información siguen sin confirmar.

Tu análisis y la primera respuesta

Cita tres hechos con sus referencias E1–E4 y dos cuestiones que requieren investigación.

Propón prioridades y acciones por rol. Explica cómo proteger la cuenta, conservar evidencias y comprobar el alcance sin retrasar una contención urgente.

Completa el registro con lo realizado en el caso y lo que propones. No anotes contraseñas ni marques una recomendación como ejecutada.

Redacta un aviso interno de cinco a ocho líneas. Indica qué ocurrió, cuándo, qué se ha hecho y qué falta comprobar.

Registro de incidentes

Identificador _____ Cuenta o activo _____ Responsable de seguimiento _____

Hora y evidencia	Hecho o decisión	Responsable	Estado y siguiente paso

Referencia y lugar autorizado de conservación de evidencias

Hechos e hipótesis y aviso interno

Continúa en otra hoja si hace falta. Entrega análisis, registro y aviso. La rúbrica valora evidencias, respuesta y roles, registro y comunicación, con un máximo de 8 puntos.