

Solución y rúbrica del caso de phishing

Guía docente del caso original de Suministros Norte. Orienta la puesta en común y la evaluación. Acepta alternativas justificadas que respeten los hechos, las responsabilidades y la protección de evidencias.

Hechos e información pendiente

E2 declara entrega de credenciales; E3 registra el aviso a las 09:06; E4 confirma a las 09:10 que informática no pidió la renovación. La cuenta de correo requiere atención prioritaria. No está confirmado un acceso al buzón ni una extracción de información.

Respuesta orientativa

La persona afectada informa por el canal interno, deja de interactuar con el mensaje y aporta la cronología sin compartir contraseñas. La comunicación temprana permite que el equipo técnico valore el riesgo.

El responsable técnico valora cambio de credenciales desde el servicio legítimo y revocación de sesiones o tokens según el sistema. Revisa accesos, métodos de recuperación, reglas de reenvío y MFA. Si hubo reutilización de la clave, identifica otras cuentas afectadas. El cambio de clave o MFA no descartan un acceso previo.

Conserva mensaje original, cabeceras y registros pertinentes con acceso autorizado; anota cada acción y resultado. La contención urgente y la preservación deben coordinarse: no esperes al final de toda la investigación para proteger la cuenta.

El alcance determina el seguimiento y las comunicaciones que procedan. El supuesto no permite afirmar una filtración ni fijar un plazo legal universal. El incidente sigue abierto hasta verificar las medidas y documentar los hallazgos.

Ejemplo de registro

Hora y evidencia	Hecho o decisión	Responsable	Estado y siguiente paso
09:06 · E3	Aviso interno: se declara entrega de credenciales.	Persona afectada y soporte	Aviso realizado. Falta investigar el uso de la cuenta.
09:10 · E4	Informática confirma que no pidió la renovación.	Soporte interno	Confirmación recibida. Valorar protección de la cuenta.
Hora por completar	Proponer cambio de credenciales, revisión y revocación de sesiones según el sistema.	Responsable técnico	Pendiente en la simulación. Registrar ejecución y resultado.
Hora por completar	Conservar correo y registros, investigar accesos y posibles cambios.	Responsable técnico	Pendiente. Documentar hallazgos y límites de la revisión.

Rúbrica de evaluación

Cuatro criterios de 0 a 2 puntos. Máximo 8. Comparte los criterios antes de comenzar y adapta el nivel técnico al grupo.

Criterio	2 puntos	1 punto	0 puntos
Evidencias	Distingue hechos e hipótesis y cita E1–E4.	Distingue parte de la información, con referencias incompletas.	Afirma accesos o daños sin evidencia.
Respuesta y roles	Prioriza protección y preservación; asigna acciones al rol adecuado y verifica resultados.	Propone medidas útiles, con responsables o seguimiento incompletos.	Omite la protección o destruye evidencias; da garantías sin comprobar.
Registro	Anota hora, referencia, decisión, responsable y estado sin contraseñas.	Faltan algunos campos o estados, pero conserva una cronología útil.	Confunde propuesta con ejecución o registra información sensible innecesaria.
Comunicación	Aviso claro, proporcional y con cuestiones pendientes y siguiente comprobación.	Aviso comprensible, con alguna omisión relevante.	No comunica o presenta hipótesis como hechos confirmados.

Ejemplo de aviso interno

A las 09:04 he introducido las credenciales de mi correo en el enlace de E1. He avisado a soporte a las 09:06 y he dejado de interactuar con el mensaje. Informática ha confirmado a las 09:10 que no pidió esa renovación. Conservo el mensaje para su revisión. Solicito valorar la protección de la cuenta y comprobar accesos y configuración. Todavía no sabemos si alguien utilizó las credenciales; las medidas técnicas propuestas están pendientes de verificar.

Adaptación y referencias

Para reducir dificultad, usa una versión en la que solo se recibe el mensaje. Para ampliarla, añade registros sintéticos y pide justificar las nuevas conclusiones. Cambia también la solución y los criterios cuando cambien las evidencias.

Material original complementario. No reproduce actividades ni el solucionario privado del manual de Paraninfo.

INCIBE · Phishing: definición y recursos de prevención
<https://www.incibe.es/aprendeciberseguridad/phishing>

INCIBE · Guía de gestión de crisis de ciberseguridad en empresas
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_gestion_de_crisis.pdf

Paraninfo · Incidentes de ciberseguridad, ISBN 9788428365413
<https://www.paraninfo.es/catalogo/9788428365413/incidentes-de-ciberseguridad>