Playbook de Respuesta ante Phishing

TechNova Solutions S.L.

---

1. Introducción

Este documento describe el protocolo oficial de TechNova Solutions S.L. ante un incidente de phishing. El objetivo es garantizar una respuesta rápida, coordinada y efectiva para minimizar el impacto, proteger los activos digitales y reforzar la seguridad posterior al incidente.

- Ámbito de aplicación: Empleados, sistemas de correo electrónico y activos digitales.
- Frecuencia de revisión: Semestral o tras un incidente relevante.

2. Escenario

Un empleado recibe un correo electrónico falso que aparenta ser de un proveedor confiable, solicitando la descarga de un archivo o la introducción de credenciales.

Ejemplo:

El martes a las 10:15h, un empleado reporta haber recibido un correo del "Departamento de IT" solicitando restablecer su contraseña mediante un enlace sospechoso.

3. Objetivos

☑ Contener el impacto del phishing inmediatamente.

☑ Identificar y aislar cuentas o sistemas comprometidos.

☑ Preservar evidencias para análisis forense.

☑ Notificar a las autoridades si procede.

☑ Reforzar la seguridad post-incidente.

☑ Mejorar la conciencia y formación de los empleados.

4. Roles y Responsabilidades

ROL	RESPONSABILIDAD
Empleado	Reportar emails sospechosos al área de IT.
IT	Analizar correos, aislar sistemas Afectados.
CISO/DPO	Coordinar la respuesta y evaluar el impacto.
Legal	Asesorar sobre comunicación externa y obligaciones legales.
Infraestructura	Revisar logs y reforzar seguridad del correo.
Proveedor de email	Colaborar en bloqueo de remitentes maliciosos.
Comunicación	Gestionar mensajes internos y externos.

5. Procedimiento de Respuesta

Fase 1: Contención Inmediata

☑ Bloquear remitente y URL sospechosa.

☑ Aislar cuentas comprometidas (reseteo de contraseña inmediato).

☑ Notificar al equipo de respuesta a incidentes.

☑ Capturar evidencia (correo original, encabezados, logs).

Fase 2: Análisis y Erradicación

☑ Analizar encabezados y adjuntos sospechosos (sandbox, antivirus).

☑ Verificar accesos indebidos en cuentas afectadas.

☑ Eliminar correos maliciosos del resto de bandejas si es necesario.

Fase 3: Recuperación

☑ Restaurar accesos seguros.

☑ Notificar a los usuarios afectados.

☑ Reforzar reglas de filtrado en gateways de correo.

Fase 4: Mejora Continua

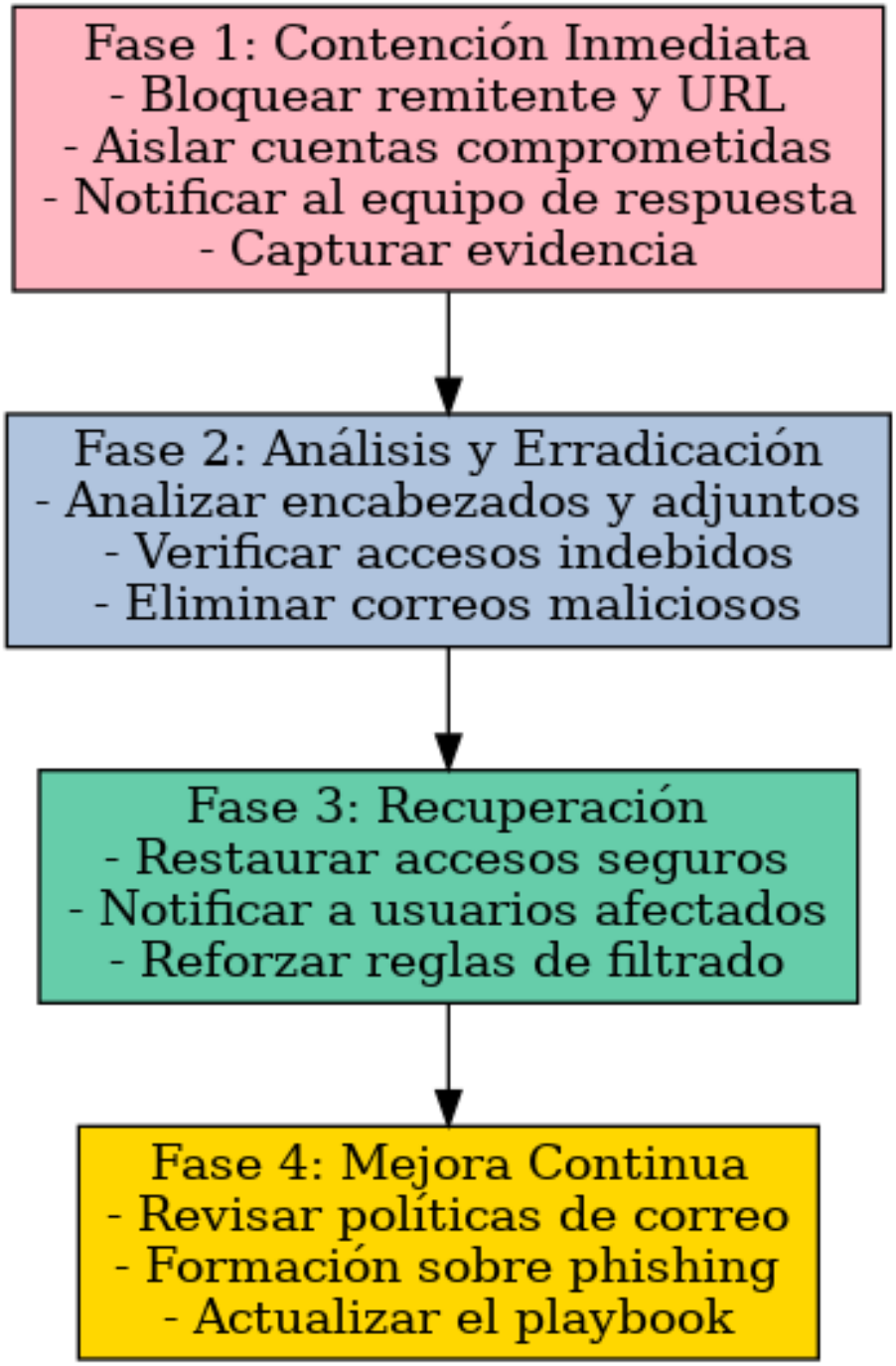
☑ Revisar políticas de seguridad del correo electrónico.

☑ Realizar formación específica sobre phishing.

☑ Actualizar este playbook según lecciones aprendidas.

6. Diagrama de Flujo del Procedimiento

A continuación se muestra el diagrama de flujo del procedimiento de respuesta:



7. Herramientas Recomendadas

FASE	HERRAMIENTA	FUNCIONALIDAD
Detección	Wazuh (SIEM)	Monitorización de eventos sospechosos (https://wazuh.com/)
Contención	Microsoft Defender for Office 365	Detección y contención automática de phisings (https://learn.microsoft.com/en-us/defender-office-365/office-365-ti)
Análisis	MXToolbox	Analizar encabezados de emails (https://mxtoolbox.com/EmailHeaders.aspx)
Análisis	VirusTotal	Analizar enlaces y archivos sospechosos (https://www.virustotal.com/gui/home/upload)
Análisis	Any.Run	Análisis dinámico de archivos adjuntos (https://any.run/)
Erradicación	(Acción manual)	Reset de contraseñas y bloqueo de cuentas comprometidas
Recuperación	(Acción manual)	Realizar accesos normales y revisar logs de actividad.
Mejora continua	(Formación interna o KnowBe 4)	Realizar campañas de formación sobre phising (https://www.knowbe4.com/)

8. Notificación a Autoridades

Debe realizarse cuando:

- Se comprometan datos personales.
- El impacto sea grave o de carácter público.

Organismos:

- INCIBE-CERT: https://www.incibe-cert.es
- AEPD: https://www.aepd.es

Datos requeridos:

- Fecha, hora y responsable.
- Tipo de incidente.
- Medidas adoptadas.
- Nº de expediente.

Ejemplo de notificación:

Fecha y hora del incidente: Martes, 27 de abril de 2025, 10:15h

Responsable: Laura Gómez, DPO - TechNova Solutions S.L.

Tipo de incidente: Phishing dirigido (correo suplantando a IT)

Alcance: 5 cuentas de correo expuestas, sin evidencias de exfiltración

Medidas adoptadas:

- Bloqueo de remitente.
- Análisis de correo en sandbox.
- Reinicio de contraseñas afectadas.
- Reforzamiento de filtros de correo.

Nº de expediente: INC-2025-0427-002

9. Prevención y Formación

☑ Campañas trimestrales de simulación de phishing.

☑ Formación continua sobre detección de correos sospechosos.

☑ Autenticación multifactor (MFA) obligatoria.

☑ Revisiones periódicas de configuraciones de correo.

☑ Modelo de acceso Zero Trust.

10. Bibliografía

INCIBE. (2024). Guía de actuación ante phishing. https://www.incibe.es

CCN-CERT. (2023). Buenas prácticas en seguridad de correo electrónico. https://www.ccn-cert.cni.es

Proofpoint. (s.f.). Email Security Best Practices. https://www.proofpoint.com

Cofense. (s.f.). Phishing Defense Guide. https://cofense.com
