networksecurityalliance

GUÍA DE ACCIÓN ANTE

PHISHING

BASADA EN *NIST*

Esta Guía de Acción ante Phishing, basada en las recomendaciones del National Institute of Standards and Technology (NIST), ofrece un enfoque técnico y práctico para identificar, responder y prevenir.

Presentado por:

networksecurityalliance

ÍNDICE
CONTENIDO

5.-Contención Inmediata

- Objetivo
- Acciones técnicas
- Comunicación interna
- Ejemplo de alerta

6.-Erradicación y Recuperación

- Objetivo
- Limpieza y restauración
- Auditoría y monitoreo posterior

7.-Lecciones Aprendidas

- Objetivo
- Revisión post incidente
- Actualización de filtros y métricas

8.-Checklist Rápido de Respuesta

9.-Recursos NIST Recomendados

10.-Plantillas Operativas

- Informe de incidente
- Correo interno de alerta

11.-Mejora Continua

- Simulaciones, métricas y capacitación

INTRODUCCIÓN

El phishing continúa siendo una de las principales amenazas en ciberseguridad, responsable de gran parte de los accesos no autorizados, filtraciones de datos y fraudes corporativos. Su éxito radica en la ingeniería social: aprovechar la confianza y el descuido humano para comprometer sistemas y credenciales.
Esta Guía de Acción ante Phishing, desarrollada con base en los lineamientos del National Institute of Standards and Technology (NIST), ofrece un enfoque técnico, estructurado y práctico para que las organizaciones puedan prevenir, detectar, responder y recuperarse eficazmente ante intentos de phishing.
El documento está diseñado para servir como una herramienta operativa que ayude a los equipos de seguridad, TI y respuesta a incidentes (CSIRT/IRT) a fortalecer su capacidad de reacción, mejorar la coordinación interna y fomentar una cultura de ciberseguridad sostenible.
A lo largo de esta guía, se presentan procedimientos paso a paso, plantillas, métricas e indicadores, así como referencias oficiales de NIST, con el fin de estandarizar las acciones y reducir el impacto de este tipo de ataques en la organización.

FASE DE PREPARACIÓN

Objetivo: reducir probabilidad e impacto.

- **Roles y responsabilidades:** asignar CSIRT/IRT, IT, Comunicaciones, Legal, RRHH.
- **Controles técnicos:** aplicar SPF/DKIM/DMARC, filtrado de correo, sandboxing de adjuntos.
- **Autenticación:** usar MFA resistente a phishing (tokens o llaves físicas).
- **Concienciación:** campañas y simulaciones calibradas con NIST *Phish Scale*.
- **Documentación:** crear playbooks específicos por tipo de phishing.

DETECCIÓN Y REPORTE

Objetivo: identificar rápido y canalizar el reporte.

- Botón “Report Phish” o correo interno.
- Monitoreo: dominios nuevos, adjuntos sospechosos, fallos SPF/DKIM.
- Reglas SIEM: alertar ante correos con adjuntos ejecutables o links nuevos.

ANÁLISIS INICIAL

Objetivo: clasificar gravedad e impacto.

- Cabeceras completas del correo.
- URLs expandidas y hash de adjuntos.
- Usuarios objetivo y acciones realizadas.
- Uso de *Phish Scale* para medir dificultad de detección.

CONTENCIÓN INMEDIATA

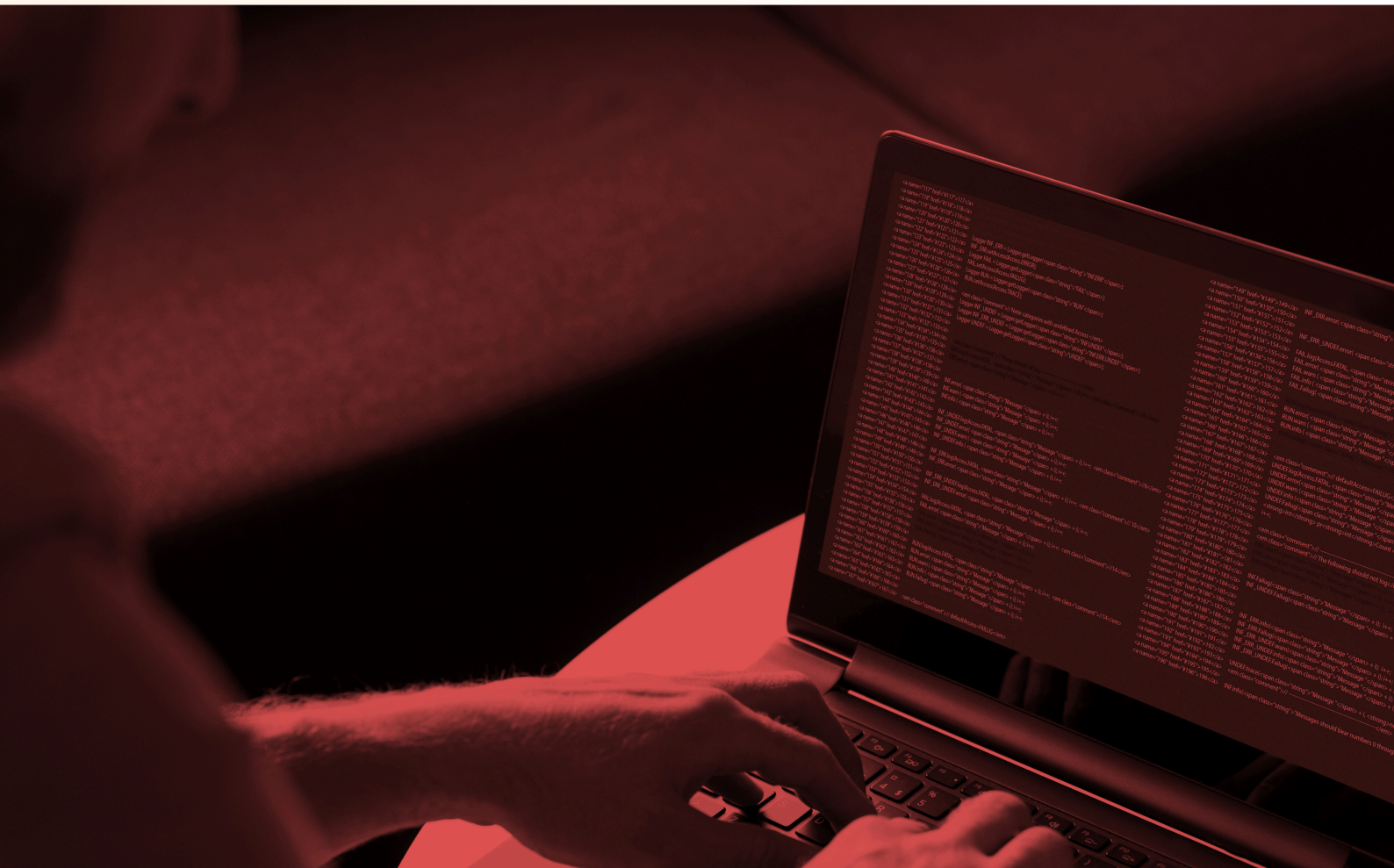
Objetivo: detener propagación.

- Reset de contraseñas y revocar sesiones.
- Bloquear remitentes, dominios y URLs en gateway/DNS.
- Aislar equipos afectados.
- Notificación interna (plantilla de alerta breve).

Ejemplo:

Asunto: Posible intento de phishing detectado

Cuerpo: “Por favor no abras el correo titulado ‘[Asunto]’. Si lo hiciste, cambia tu contraseña y contacta a IT de inmediato.”



ERRADIACIÓN Y RECUPERACIÓN

Objetivo: eliminar rastros y restaurar operaciones seguras.

- Limpieza de malware o cuentas comprometidas.
- Auditoría de accesos y privilegios.
- Cambio de contraseñas/tokens/API.
- Monitoreo reforzado 14 días.

LECCIONES APRENDIDAS

Objetivo: prevenir repetición.

- Reunión post mortem (72h).
-
- Actualizar filtros, playbooks y capacitación.
-
- Métricas: tasa de reporte, tasa de click, tiempo de detección (MTTD), tiempo de respuesta (MTTR).

CHECK LIST RÁPIDO

1. Guardar correo original.
2. Extraer cabeceras, URLs y adjuntos.
3. Verificar si hubo acceso o descarga.
4. Bloquear remitente/dominio.
5. Reset contraseñas.
6. Aislar endpoints.
7. Notificar.
8. Analizar y documentar.

PLANTILLAS

Informe de incidente:

- Fecha/hora:
- Tipo: (spear, credenciales, malware)
- Usuarios afectados:
- Acciones inmediatas:
- Estado actual:

Correo interno:
Asunto: Acción requerida por intento de phishing
Cuerpo: “Se detectó un correo fraudulento. Cambia tu contraseña y reporta si lo abriste.”

MEJORA CONTINUA

- Simulaciones periódicas basadas en *Phish Scale*.
-
- Actualización mensual de indicadores de riesgo.
-
- Capacitaciones trimestrales anti-phishing.

REFERENCIA: BASADO EN LINEAMIENTOS NIST SP 800-61R2, TN 2276 (PHISH SCALE), SP 800-177 Y MATERIALES NIST PARA PYMES.

CONTACTO

55-39-33-56-60
networksecurityalliance.com
Canadá 177, San Lucas, Coyoacán,
04030 Ciudad de México, CDMX