Metodología de Phishing Ético

Guía de trabajo para programas de concientización,medición y mejora continua en organizaciones.

> **Uso permitido:** este documento describe un enfoque **defensivo** y **autorizado** para simulaciones internas de ingeniería social. No contiene instrucciones para actividades maliciosas. Toda ejecución debe realizarse con aprobación formal y controles de seguridad.

I3G Ciberseguridad
Sitio web: i3g.cl

Versión: v1.0 (2026)

Resumen ejecutivo

El phishing sigue siendo una de las vías más frecuentes para iniciar incidentes de seguridad:

Un solo clic puede abrir la puerta a robo de credenciales, acceso no autorizado y movimientos laterales.
El phishing ético es una práctica controlada y legal que permite evaluar el nivel de exposición humana, medir comportamientos y reforzar hábitos seguros mediante aprendizaje inmediato.

La metodología de **I3G** se basa en campañas periódicas, seguras y medibles, combinadas con capacitación breve y recomendaciones técnicas. El objetivo no es “atrapar” a las personas, sino reducir el riesgo, mejorar la detección temprana y fortalecer la cultura de seguridad.

Qué obtienes con este enfoque

- Visibilidad real del riesgo humano: clics, reportes y tiempos de reacción.
- Aprendizaje inmediato: retroalimentación en el momento y micro-capacitaciones.
- Evidencia para auditorías y mejoras: reportes y recomendaciones accionables.
- Mejora continua: reducción de reincidencia y aumento de reporte responsable.

Principios del phishing ético (I3G)

- **Legalidad y autorización**: toda campaña requiere aprobación formal del cliente y definición de alcance.
- **No daño**: no se entrega malware, no se busca interrumpir operaciones, no se accede a información sensible.
- **Privacidad por diseño**: minimización de datos, acceso restringido y retención limitada.
- **Transparencia posterior**: cierre educativo, explicación del escenario y buenas prácticas.
- **Mejora continua**: ajustes por áreas, roles y riesgos reales del negocio.

Alcance y roles

Antes de iniciar,se define un alcance claro para asegurar que la simulación sea segura, justa y útil.

Definiciones clave

- **Población objetivo**: áreas incluidas/excluidas, nuevos ingresos, terceros (si aplica).
- **Canales**: correo corporativo (principal) y otros canales solo si están aprobados (mensaje interno).
- **Ventana de campaña**: periodo de ejecución y horarios para minimizar impacto operativo.
- **Qué se mide**: apertura/clic/reporte, interacción con página educativa, respuesta ante alerta.
- **Qué NO se hace**: solicitudes reales de contraseña, cobros, enlaces a descargas, ni suplantación de autoridades sensibles.

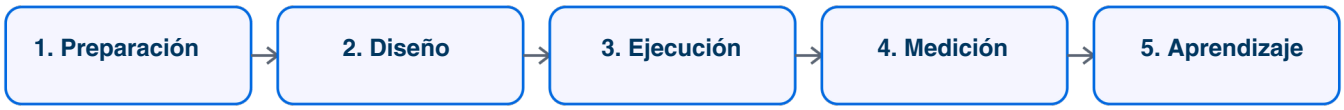
Roles recomendados

Rol	Responsabilidad
Cliente	Aprueba objetivos, alcance y comunicación interna.
TI / Seguridad	Valida listas, controles, canal de reporte y coordinación.
RR.HH. / Comunicaciones	Entrega la nómina vigente de colaboradores y sus correos para asegurar un alcance correcto.
I3G (equipo ejecutor)	Diseño, ejecución controlada, medición, reporte y capacitación.

Recomendación: definir un canal único de reporte (por ejemplo, botón o buzón) y un flujo de atención. Aumenta la tasa de reporte y reduce la incertidumbre cuando aparece un correo sospechoso.

Metodología I3G: fases del programa

Flujo de trabajo (vista simplificada)



Fase 1 - Preparación y línea base

- Levantamiento de contexto: amenazas comunes para la industria y procesos críticos.
- Definición de indicadores y metas realistas (cultura, reporte, respuesta).
- Aprobaciones, comunicaciones y reglas de juego (qué se mide y cómo se usa).
- Configuración de controles: listas, remitentes autorizados y páginas educativas.

Fase 2 - Diseño de escenarios realistas

Se crean escenarios creíbles alineados al día a día del negocio (por ejemplo, logística, recursos humanos, plataformas internas o e-commerce), manteniendo un estándar de respeto y evitando temas sensibles.

- Nivel de dificultad progresivo: desde señales evidentes hasta patrones más sutiles.
- Mensajes consistentes con la cultura y lenguaje interno.
- Elementos de aprendizaje: señales de alerta y práctica del reporte.

Fase 3 - Ejecución controlada

- Envío segmentado y monitoreo continuo para responder ante dudas.
- Páginas de destino educativas (sin recolección innecesaria de datos).
- Registro de eventos de interacción para análisis posterior.

Seguridad por defecto: las simulaciones no incluyen archivos ejecutables ni enlaces de descarga, y se diseñan para no poner en riesgo la operación. El objetivo es medir y educar, no probar límites técnicos.

Medición, reporte y aprendizaje

Los resultados se analizan deforma agregada y orientada a mejora.
Cuando se revisan casos individuales, se hace con criterios acordados previamente y enfoque formativo.

Indicadores sugeridos

- **Tasa de interacción:** clics y acciones en la página educativa.
- **Tasa de reporte**: usuarios que reportan el correo sospechoso por el canal definido.
- **Tiempo a reporte**: cuánto demora el primer reporte desde el envío.
- **Reincidencia**: repetición de clic en campañas sucesivas (útil para refuerzo).
- **Cobertura**: participación por área, rol o sede (sin exponer públicamente a personas).

Entregables de I3G

- Plan de campaña y alcance aprobado (objetivo, público, calendario, métricas).
- Simulación controlada + páginas educativas de refuerzo.
- Reporte ejecutivo (hallazgos, tendencias, puntos críticos).
- Recomendaciones prácticas: hábitos de verificación y controles técnicos complementarios.
- Material de capacitación breve (microlearning) para reforzar lo aprendido.

Fase 4 - Capacitación y refuerzo

Cada campaña termina con una devolución clara: qué señales se observaron, por qué el escenario era riesgoso y cómo actuar en adelante.

- La capacitación se adapta al nivel de madurez del equipo.
- Mensajes breves y prácticos (orientados a acción).
- Recordatorios de “qué hacer” ante dudas: pausar, verificar, reportar.
- Contenido específico para perfiles de mayor riesgo (por ejemplo, finanzas o compras).

Fase 5 - Mejora continua

- Ajuste de escenarios según resultados y nuevas amenazas.
- Plan de refuerzo para áreas con mayor exposición.
- Revisión de controles técnicos (MFA, filtros, reportes, bloqueo de dominios sospechosos).

Gobernanza, privacidad y seguridad de los datos

- **Minimización**: se recopilan solo los datos necesarios para medir el programa.
- **Acceso restringido**: resultados disponibles solo para responsables definidos.
- **Retención limitada**: plazos acotados según política interna y acuerdos.
- **Anonimización**: reportes por área/rol cuando sea posible.
- **Comunicación responsable**: foco en aprendizaje, no en sanción.

> **Nota:** la efectividad del programa aumenta cuando se combina con controles técnicos (MFA, filtrado, EDR) y con un canal de reporte simple. La concientización no reemplaza la seguridad técnica: la complementa.

Preguntas frecuentes

Pregunta	Respuesta
¿Esto es legal?	Sí, siempre que exista autorización formal, alcance definido y controles que eviten daño. I3G trabaja bajo acuerdos y reglas de ejecución aprobadas.
¿Se exponen nombres de personas?	No. El estándar recomendado es reportar de forma agregada y formativa. Cualquier revisión individual debe estar acordada previamente.
¿Con qué frecuencia se recomienda?	Programas periódicos permiten medir mejora. La frecuencia se ajusta a la madurez de la organización y a la carga operativa.
¿Qué pasa si alguien reporta un correo real?	Se aprovecha como oportunidad de aprendizaje y se refuerza el canal de reporte. El objetivo es aumentar la detección temprana.
¿Con diferencia esto de un Pentesting?	El phishing ético mide y entrena comportamientos humanos y procesos de reporte. El pentesting evalúa controles técnicos mediante pruebas especializadas.

Contacto

Si quieres implementar un programa de phishing ético con enfoque educativo con evidencia y accionable, conversemos sobre el alcance y el nivel de madurez de tu organización.

Web: i3g.cl | **Contacto:** i3g.cl/contacto

I3G Ciberseguridad, tu tranquilidad digital nuestra mayor responsabilidad.