

# 1. Socialización de resultados del ejercicio de Ingeniería Social. 01 de diciembre de 2025.

**CONTENIDO**

1. Programación
2. Ejecución de la simulación
3. Email campaña
4. Resultados de la simulación
5. Oportunidades de mejora

**Descripción**

El tercer ejercicio 2025 de simulación consistió en el envío masivo de un correo electrónico desde una dirección falsificada: **ComunicadosADRES@gov.com**, simulando ser una comunicación institucional legítima de la entidad.

El mensaje, con asunto "Encuesta de Rendición de Cuentas 2024 - 2025", invitaba a los usuarios a participar de una encuesta de satisfacción luego del evento de rendición de cuentas.

La técnica utilizada se basó en la suplantación de una comunicación corporativa interna y en la limitación de un proceso legítimo de autenticación en Microsoft. El contenido de mejora organizacional y la apariencia institucional del mensaje aumentaban la probabilidad de que los destinatarios confiaran en la legitimidad de la solicitud.

**Población Objeto:** 700 cuentas de correo electrónico de usuarios pertenecientes a la ADRES.

**Escenario:** Virtual, utilizando Microsoft 365 Defender mediante el envío masivo de correos.

Cabe señalar que no se puso en riesgo la integridad de los usuarios (Remitentes Públicos ni contristas), por lo tanto, la simulación no presenta ninguna amenaza para la ADRES.

**Envío del correo**

- Cada usuario objetivo recibió en su bandeja de entrada un correo con el asunto "Encuesta de Rendición de Cuentas 2024 - 2025", enviado desde una cuenta falsificada identificada como: **ComunicadosADRES@gov.com**
- En el cuerpo del correo se incluyó la invitación a participar en la encuesta de satisfacción, acompañada de un enlace al supuesto formulario. Antes de poder diligenciarlo, el usuario debía autenticarse en un portal falso que imitaba la página de inicio de sesión de Microsoft, momento en el que se capturaban las credenciales ingresadas.

**Correo electrónico - mensaje**

- El mensaje incluía un componente visual con formato limpio y corporativo, acompañado de un botón identificado como "Responder encuesta de satisfacción", que redirigió a una página intermedia bajo la apariencia del ingreso a Microsoft "Ingreso de credenciales". Esta página daba a entender que para contestar la encuesta se debía registrar con el usuario y contraseña de dominio ADRES.

**Comparativo de simulaciones**

**USUARIOS COMPROMETIDOS**

Fecha	Usuarios comprometidos
SEP_23_2025	115
SEP_24_2025	385
SEP_25_2025	385
SEP_26_2025	385
SEP_27_2025	385
SEP_28_2025	385
SEP_29_2025	385
SEP_30_2025	385
SEP_31_2025	385

**MENSAJES LEIDOS**

Fecha	Mensajes Leídos
SEP_23_2025	577
SEP_24_2025	387
SEP_25_2025	387
SEP_26_2025	387
SEP_27_2025	387
SEP_28_2025	387
SEP_29_2025	387
SEP_30_2025	387
SEP_31_2025	387

**MENSAJES ELIMINADOS**

Fecha	Mensajes Eliminados
SEP_23_2025	115
SEP_24_2025	385
SEP_25_2025	385
SEP_26_2025	385
SEP_27_2025	385
SEP_28_2025	385
SEP_29_2025	385
SEP_30_2025	385
SEP_31_2025	385

**MENSAJES REENVIADOS**

Fecha	Mensajes Reenviados
SEP_23_2025	8
SEP_24_2025	8
SEP_25_2025	8
SEP_26_2025	8
SEP_27_2025	8
SEP_28_2025	8
SEP_29_2025	8
SEP_30_2025	8
SEP_31_2025	8

**Sugerencias de seguridad**

1. Revisar o analizar las direcciones de correo electrónico o los dominios oficiales de la entidad. (.com)
2. Verificar con el personal de soporte de la ADRES o realizar un escalamiento por mesa de servicio, buscando indagar la veracidad del correo. (No reenviar)
3. Desconfiar y cerciorarse de aquellas páginas o links que soliciten el ingreso de usuarios y contraseñas.

**Asignaciones de aprendizaje**

**Sumate a la seguridad digital**

Participa en el primer taller de capacitación de seguridad digital. Este taller te ayudará a fortalecer tus conocimientos sobre seguridad digital y a tomar medidas preventivas para proteger tus datos y dispositivos.

- Duración: 1 hora
- Fecha de realización: 2 de diciembre
- Trabajo a distancia - 7 min

**Centro de conocimiento de seguridad**

**Centro de Conocimiento en ciberseguridad**

ADRES

Este repositorio centralizado almacena documentos como artículos de conocimiento, boletines, informes y presentaciones con los técnicos y técnicos de ingeniería social.

Este repositorio centralizado almacena documentos, ya sea en el formato entregado por correo o por documentos almacenados desde la DOTIC.

Las unidades de más documentos por parte de los funcionarios serán para: seguridad, personal y responder a los ataques de ingeniería social, fortaleciendo la resiliencia en el ámbito digital.

<https://www.cloud.microsoft/ORNnmf09HyXZ4L?ref=Link>

FORMATO DE CUENTA FINAL Y CARGUE EN ERP - OBLIGATORIO:reunión Calendar

Evento

Asistente para programación

Eliminar

Reiniciar

Responder a todos

Evento duplicado

Unirse

Aceptado

Proponer nueva hora

Responder

Ocupado

15 minutos antes

Clasificar

Privado

Programando sonido

11

FORMATO DE CUENTA FINAL Y CARGUE EN ERP - OBLIGATORIO

Unirse

Chatar

12

Mar 2/12/2023, de 14:30 a 16:30

13

Reunión de Microsoft Teams

14

Buenos días,

15

SOLO PARA CONTRIBUYENTES

16

Microsoft Teams

Reservita prueba

Unirse a la reunión ahora

Id. de reunión: 234 871 257 638 1

Código de acceso: xBWS9H

17

Marcar por teléfono

+57 301 1162099 380099796 Colombia, Bogotá

Reservita prueba

Id. de conferencia telefónica: 280 090 8754

18

Para organizadores: [Quitar de la reunión](#) | [Reservita prueba en FPN de masado](#)

19

Resumen de la reunión

Resumen del contenido

Archivos

4/2 Transcripciones

Seguimiento

Organizador

1

Luz Adriana Melo Sal.

Enviado el Viernes, 2/12/2023 a las 8:10

Asistentes

Se respuesta fue: "Reservita"

✓

Sin respuesta 1

2

DDP Generar

Organizadora

