Nro. Alerta:	EC-2025-056	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	31-oct-2025	**Campaña de información de Suplantación de Identidad al Ministerio de Inclusión Económica y Social - MIES**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Fraude – Phishing
Tipo de incidente: Suplantación de identidad.
Nivel de riesgo: Alto

II. INTRODUCCIÓN

El Phishing es un ciberataque donde los delincuentes envían mensajes de texto, audio, video, correos, sitios web entre otros medios de manera engañosa para que las víctimas divulguen información personal o financiera. A menudo se hacen pasar por entidades legítimas como bancos, instituciones de gobierno, operadoras del servicio móvil avanzado o tiendas, creando un sentido de urgencia para que el usuario haga clic en enlaces maliciosos y descargar archivos adjuntos que contienen malware.

El malware, o "software malicioso", es cualquier programa informático diseñado para infiltrarse en un sistema, dañar dispositivos o redes, o robar datos sin el consentimiento del usuario. Se trata de una categoría amplia que incluye virus, gusanos, ransomware, spyware y troyanos, y los ciberdelincuentes lo usan para obtener acceso no autorizado, robar información valiosa como credenciales bancarias, extorsionar a las víctimas o interrumpir servicios esenciales

III. VECTOR DE ATAQUE:

Los atacantes registran dominios y páginas que imitan la imagen institucional del Ministerio de Inclusión Económica y Social - MIES (logo, estilos, textos institucionales) y las promueven mediante enlaces en redes sociales, mensajes instantáneos y correos electrónicos.

Las páginas fraudulentas anuncian un “bono” de USD 1,000 y operan bajo dos objetivos principales:

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

1. Inducir al visitante a introducir datos personales y bancarios en formularios falsos;
2. Requerir un pago o depósito previo como condición para el desembolso.

En algunos casos la página redirige a portales de pago controlados por los atacantes y solicitan la carga de documentos escaneados para “verificación”. El flujo típico del fraude es:

a) Creación y registro de dominio parecido al oficial
b) Clonación parcial de contenido y uso de elementos visuales del MIES.
c) Difusión mediante mensajería masiva, publicaciones pagadas, cuentas falsas o enlaces en campañas de redes.
d) Captura de credenciales, datos personales, información bancaria y/o solicitud de pago.
e) Retiro de fondos, uso de datos para fraude secundario o venta en mercados ilícitos.

IV. INDICADORES DE COMPROMISO:

- **Página de Telegram:**

  MIES BONOS - https://t.me/s/bonosel

- **Sitios web:**

  https://login.miesbonos2025.com/login

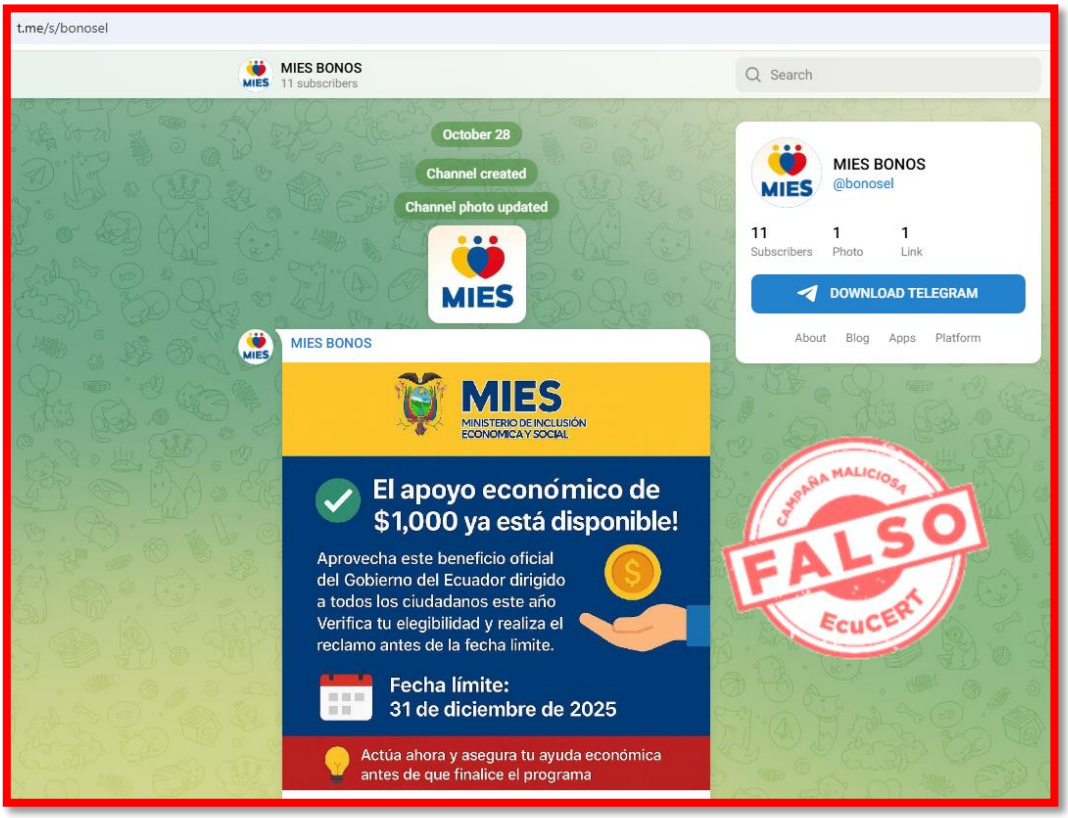
- **Direcciones Ip:**

  149.154.167.99
  75.2.60.68

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	EC-2025-056	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	31-oct-2025	**Campaña de información de Suplantación de Identidad al Ministerio de Inclusión Económica y Social - MIES**	V 1.1

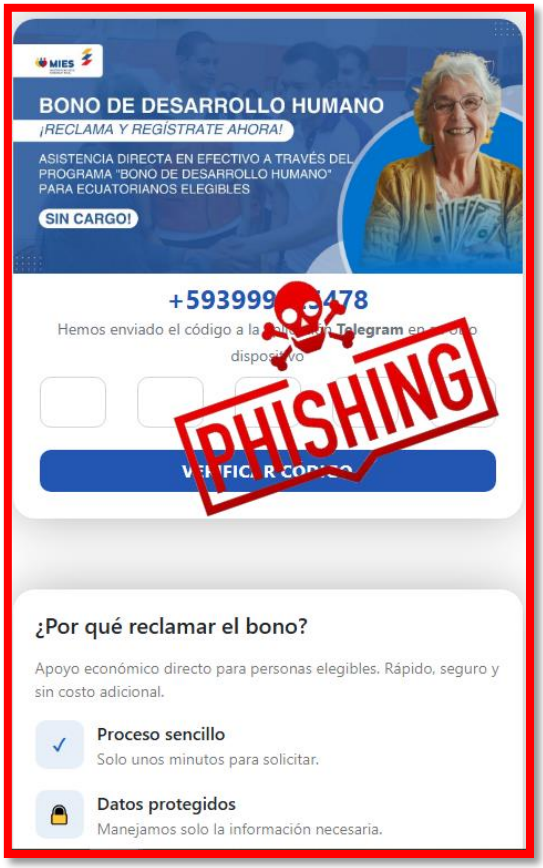
V. IMÁGENES DE LA CAMPAÑA DE SMISHING.



Gráfica 1.- Página de Telegram que suplanta el nombre del MIES.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	EC-2025-056	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	31-oct-2025	**Campaña de información de Suplantación de Identidad al Ministerio de Inclusión Económica y Social - MIES**	V 1.1



Gráfica 2.- Sitio web que suplanta el nombre del MIES.

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Validar si los sitios web en los que se navega son seguros (se utiliza el puerto https) y oficiales (el dominio corresponde a instituciones públicas, no tiene errores ortográficos).
- Hacer caso omiso a correos, links o mensajes de dudosa procedencia y márcalos como spam o bloquearlos y comunicar a su departamento técnico.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	EC-2025-056	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	31-oct-2025	**Campaña de información de Suplantación de Identidad al Ministerio de Inclusión Económica y Social - MIES**	V 1.1

- Si proporcionó claves o PIN: Cambiar inmediatamente (banco, correo, cuentas importantes).
- Si realizó depósitos: Contacte al banco inmediatamente y solicite bloqueo/cambio de tarjetas y revisión de transacciones.
- Reporte el caso al Ministerio involucrado (canales oficiales) y a la Policía Nacional
- Si compartió documentos de identidad: presente la denuncia en la Fiscalía General del Estado y proceda a solicitar a la entidad emisora un nuevo documento de identidad.
- Guarde evidencias: capturas de pantalla del sitio, URLs, correos y números.
- Revise su estado de cuenta y reporte cargos sospechosos.
- Considere presentar una denuncia formal en la unidad de delitos informáticos de la Fiscalía General del Estado.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec