Nro. Alerta:	AL-2026-006	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	07-feb-2026	Suplantación de Identidad a Sitio Web del Servicio de Rentas Internas - SRI	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Suplantación de Identidad
Tipo de Incidente: Phishing - Captura fraudulenta de Credenciales
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Sitio Web suplantado del SRI

Sitio web fraudulento que se encuentra suplantando la identidad del Servicio de Rentas Internas - SRI

III. INTRODUCCIÓN

La suplantación de identidad de un Sitio Web (también conocida como Web Spoofing o Phishing) es una técnica maliciosa en la que un ciber atacante crea una copia casi idéntica de un Sitio Web legítimo para engañar a los usuarios.

El objetivo principal es que la víctima confíe en el sitio falso y entregue voluntariamente información confidencial, como contraseñas, números de tarjetas de crédito o datos personales.

El dominio reportado https://srihome-ec[.]com, imita la imagen, denominación y funcionalidad del portal oficial del Servicio de Rentas Internas SRI, lo cual podría inducir a error a los ciudadanos y a ser utilizado para la captura fraudulenta de credenciales, información personal y/o datos financieros.

Este comportamiento corresponde a un ataque de Phishing por Suplantación de Identidad de una entidad gubernamental, representando un riesgo significativo para la Seguridad de la Información y la confianza digital de la ciudadanía.

IV. VECTOR DE ATAQUE

Acceso a un sitio Web fraudulento que pretende suplantar al sitio web del Servicio de Rentas Internas – SRI

Dominio fraudulento detectado:

- https://srihome-ec[.]com

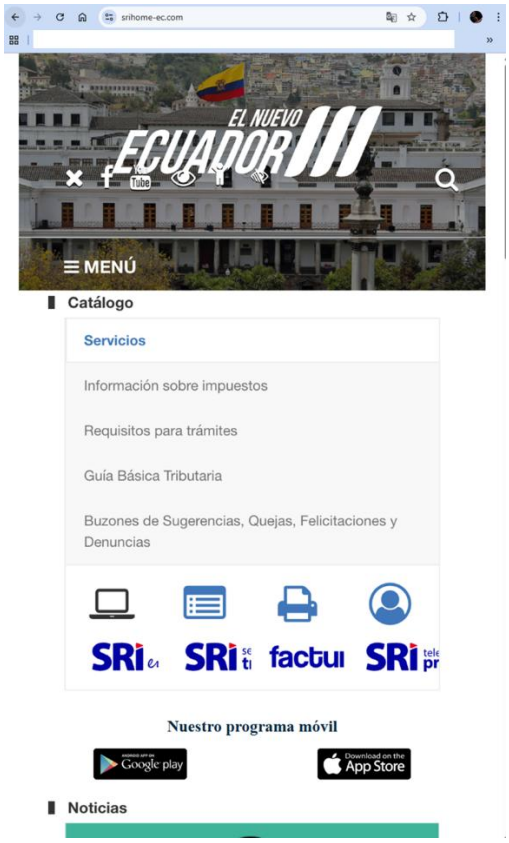

Figura 2.- Sitio Web suplantado del SRI - https://srihome-ec[.]com

Sitio web legítimo suplantado:

- https://www.sri.gob.ec

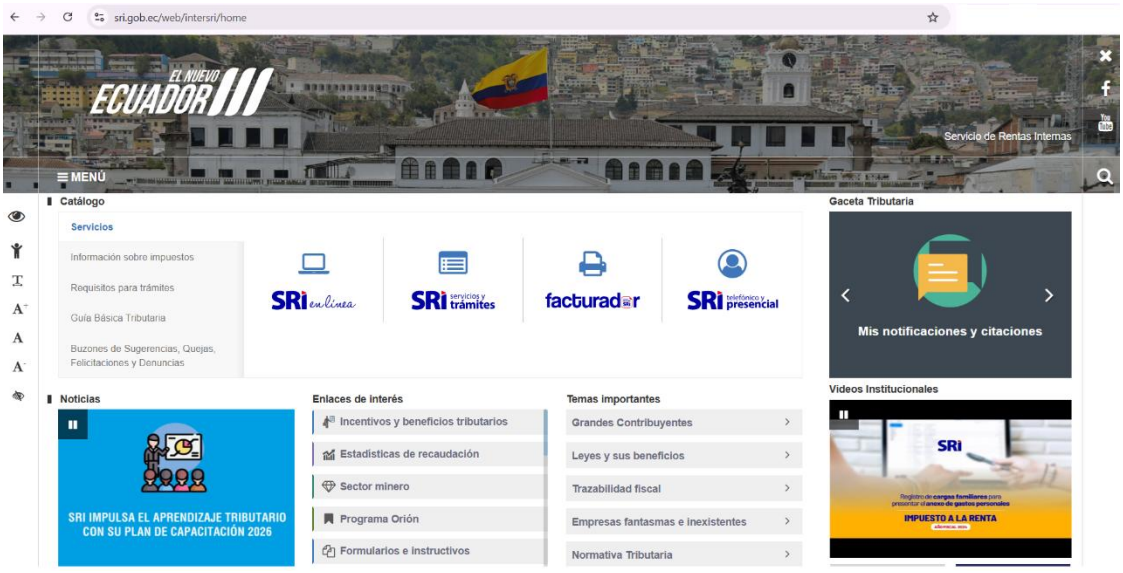

Figura 3.- Sitio Web original del SRI - https://www.sri.gob.ec/web/intersri/home

V. IMPACTO

El SRI maneja el RUC (Registro Único de Contribuyentes) y la Clave de Acceso. Si un atacante obtiene esto, puede:

- **Emitir facturas falsas:** Utilizar un perfil para declarar ventas inexistentes y lavar dinero o cometer fraudes fiscales a nombre del usuario.
- **Modificar declaraciones:** Alterar registros para generar multas o desviar devoluciones de impuestos hacia cuentas bancarias de terceros.
- **Acceso a datos patrimoniales:** Conocer ingresos, propiedades y vehículos registrados, de un usuario, lo que puede derivar en extorsiones dirigidas.
- **Ingresar datos crediticios** creyendo que está pagando una multa o matrícula vehicular.
- **Realizar transferencias directas** a cuentas de delincuentes pensando que son cuentas institucionales.
- **Indefensión:** Si el atacante altera información, el SRI legalmente le hará responsable de esos cambios hasta que se logre demostrar el hackeo.

- **Multas reales por trámites no realizados:** El ciudadano cree que ya cumplió con su declaración en la web falsa, pero ante el sistema real está en mora, lo que genera intereses y recargos reales.

- **A nivel social**, la suplantación masiva **genera un clima de inseguridad digital**. La ciudadanía comienza a temer realizar trámites en línea, lo que ralentiza la digitalización del país y satura las agencias físicas del SRI por miedo a ser estafados en la Web.

VI. INDICADORES DE COMPROMISO

- **Dominios sospechosos detectados en 2025-2026:**

Indicador	Tipo	Contexto
srihome-ec[.]com	Nombre de dominio	Sitio Web fraudulento
104.21.95.144	Dirección IP	IP v4
006d145e2cd492d72278e48ec77cc29edadd6f0280f9fda-debad029a7cddb27c	Hash	SHA-256

VII. RECOMENDACIONES:

- Antes de introducir cualquier dato en un navegador de internet, observar la barra de direcciones. Los ciber atacantes usan Typosquatting (Por ejemplo, g0ogle.com en lugar de google.com) o dominios similares, para el causo identificar que el sitio original del SRI es https://sri.gob.ec y no srihome-ec.com. Si el enlace parece una sopa de letras o no coincide exactamente con el sitio oficial, salir de ahí.

- El Phishing vive de las emociones. Considerar que si recibe un mensaje que dice: "Tu cuenta será bloqueada en 1 hora" o "Acceso no autorizado detectado, actúa ya", es una señal de alerta roja. Las entidades serias rara vez usan tácticas de pánico.
- Implementar el MFA (Doble Factor de Autenticación), es la mejor línea de defensa. Incluso si un ciber atacante obtiene tu contraseña a través de un sitio web falso, no

podrá acceder sin el código temporal de una App de autenticación (como Google Authenticator) o una llave física.

- Los gestores de contraseñas (como Bitwarden o 1Password) son excelentes detectores de Phishing: no autorrellenarán sus datos si la URL del sitio no coincide exactamente con la guardada en su base de datos.

- El protocolo HTTPS (el candado) significa que la conexión es cifrada, pero hoy en día la mayoría de los sitios de Phishing también tienen certificados SSL. El candado garantiza que nadie "escucha", pero no garantiza que el dueño del sitio sea quien dice ser.

- Si identifica un intento de suplantación, no solo borre. Utilice las herramientas de "Reportar Phishing" de su cliente de correo. Esto ayuda a los filtros de IA a aprender y proteger a otros usuarios.

- Muchos sitios fraudulentos aprovechan vulnerabilidades del navegador para ejecutar código. Tener su navegador y sistema operativo al día garantiza que los parches de seguridad más recientes estén activos.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.

- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.

- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- **SRI (2026).** *Servicio de Rentas Internas*. https://www.sri.gob.ec/web/intersri/home