Nro. Alerta:	AL-2025-055	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	TLP:BLANCO	**ALERTAS DE SEGURIDAD**	ecucert
Fecha:	21-oct-2025	**Suplantación de Identidad "Registro Civil"**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Fraude – Vishing

Tipo de incidente: Falsificación de registros o identidad.

Nivel de riesgo: Alto

II. INTRODUCCIÓN

El Phishing a través de llamadas telefónicas, conocido como Vishing, es una forma de ciberataque donde los delincuentes se comunican con la victima para incitar a revelar información confidencial personal o financiera, instalar aplicativos de dudosa procedencia u otros tipos de engaños.

Generalmente, los atacantes se hacen pasar por entidades legítimas, como instituciones públicas, entidades bancarias, operadoras del servicio móvil avanzado o establecimientos comerciales. A menudo crean un sentido de urgencia o alarma para que el usuario proporcione información, haga clic en enlaces maliciosos o descargue archivos adjuntos que contienen software malicioso (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:

A través de llamadas telefónicas, los atacantes se hacen pasar por funcionarios de la Dirección General de Registro Civil, Identificación y Cedulación ofrecen soporte para la instalación del servicio de cédula digital en el teléfono celular del ciudadano.

Durante la llamada, si el ciudadano acepta la asistencia, los atacantes le proporcionan un número de teléfono móvil al que debe enviar la palabra "Asesor", junto con un código identificado como "C24". Una vez que el ciudadano envía el mensaje, recibe una nueva llamada en la que los delincuentes le indican los pasos

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

incidente@ecucert.gob.ec @ecucert_ec www.ecucert.gob.ec

Nro. Alerta:	AL-2025-055	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	ecucert
TLP:	TLP:BLANCO	**ALERTAS DE SEGURIDAD**	
Fecha:	21-oct-2025	**Suplantación de Identidad "Registro Civil"**	V 1.1

para instalar una aplicación maliciosa (APK) con el nombre GOB.ec, la cual se encuentra disponible en el sitio web fraudulento: https://registrocivil-gob.com/

IV. INDICADORES DE COMPROMISO:

El indicador de compromiso reportado y asociado a la campaña maliciosa son los enlaces que dirigen a los sitios web fraudulentos:

- ***Sitios web:***

  https://registrocivil-gob.com/

- ***Números de teléfono:***

  098 700 0150
  02 594 8142
  02 209 6617
  02 046 3144
  02 904 1592

V. IMÁGENES DE LA CAMPAÑA DE SUPLANTACIÓN DE IDENTIDAD.

Gráfica 1.- Sitio web que suplanta a la aplicación "GOB.EC a través del sitio https[:]//registrocivil.gob.com"

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
incidente@ecucert.gob.ec @ecucert_ec www.ecucert.gob.ec

Nro. Alerta:	AL-2025-055	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-oct-2025	**Suplantación de Identidad "Registro Civil"**	V 1.1

VI. SITIO WEB REAL DE LA DIRECCIÓN GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN

https://apps.registrocivil.gob.ec/

Gráfica 2.- Información en Página WEB real del Registro Civil

VII. 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 al nombre de la empresa, 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.
- Ante cualquier duda contactarse directamente con la persona o empresa suplantada para su comprobación y/o denuncia.

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
incidente@ecucert.gob.ec @ecucert_ec www.ecucert.gob.ec

Nro. Alerta:	AL-2025-055	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	TLP:BLANCO	**ALERTAS DE SEGURIDAD**	ecucert
Fecha:	21-oct-2025	**Suplantación de Identidad "Registro Civil"**	V 1.1

- En caso de haber ingresado los datos personales en el sitio web fraudulento, cambiar la contraseña de las cuentas y comunicarse inmediatamente con la empresa suplantada para la toma de acciones de remediación.
- Nunca entregue los usuarios y contraseñas solicitados a través de correos electrónicos, redes sociales o llamadas telefónicas.
- Instalar y mantener actualizado una solución Antivirus.
- Bloquear los sitios web o direcciones de correo electrónicos indicados en la sección indicadores de compromisos.
- Mantenerse informado continuamente sobre tipos de amenazas en el internet.
- Si es necesario instalar archivos .apk en su dispositivo descargarlo sólo de fuentes confiables como Google Play Store, AppGallery, Galaxy Store u otras tiendas oficiales.

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
incidente@ecucert.gob.ec @ecucert_ec www.ecucert.gob.ec