Nro. Alerta:	AL-2026-014	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **Aviso de seguridad**	ecucert
TLP:	TLP:CLEAR		
Fecha:	23-mar-2026	**Abuso de plataforma elearning.trabajo.gob.ec para envío de SPAM**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Email Security Incident / SPAM Abuse

Tipo de incidente: Abuso de servicio / posible compromiso de cuenta institucional

Nivel de riesgo: Alto

II. INTRODUCCIÓN

El abuso de cuentas institucionales para el envío de correos electrónicos no solicitados (SPAM) constituye una amenaza relevante en el ámbito de la ciberseguridad, ya que puede ser indicio de compromiso de credenciales o uso indebido de plataformas legítimas.

En este tipo de incidentes, los atacantes o actores maliciosos utilizan infraestructuras confiables para distribuir mensajes masivos, incrementando la probabilidad de que los correos sean abiertos por los destinatarios. Cuando estos correos provienen de dominios oficiales, como entidades gubernamentales, generan un alto nivel de confianza en los usuarios, facilitando posibles ataques posteriores como phishing, robo de credenciales o campañas de desinformación.

Este tipo de eventos puede estar asociado a vulnerabilidades en sistemas internos, abuso de funcionalidades como recuperación de contraseñas o notificaciones automáticas, o compromisos parciales de plataformas tecnológicas. Para eso es fundamental realizar análisis técnicos oportunos y aplicar medidas de mitigación adecuadas.

III. VECTOR DE ATAQUE:

Se ha detectado un posible compromiso o abuso de la cuenta institucional noreply_elearning@trabajo.gob.ec, perteneciente a la plataforma de capacitación del Ministerio del Trabajo, la cual estaría siendo utilizada para la distribución de correos no solicitados (SPAM).

El evento fue reportado por un miembro de la comunidad académica y analizado preliminarmente.

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:	AL-2026-014	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **Aviso de seguridad**	ecucert
TLP:	TLP:CLEAR		
Fecha:	23-mar-2026	**Abuso de plataforma elearning.trabajo.gob.ec para envío de SPAM**	V 1.1

Características del correo detectado:

- **Asunto:** “Nuevo inicio de sesión con tu cuenta Ministerio del Trabajo”
- **Remitente mostrado (display):** noreply_elearning@trabajo.gob.ec
- **Remitente real (From):** noreply_elearning@trabajo.gob.ec

Infraestructura de envío identificada:

- **IP origen:** 190.152.44.225
- **Hostname:** spf24.trabajo.gob.ec
- **Proveedor:** CNT EP (AS28006)
- **Ubicación:** Quito – Ecuador

De acuerdo con los registros analizados, el mensaje fue entregado desde infraestructura legítima asociada al dominio trabajo.gob.ec, lo que sugiere un posible abuso de la plataforma de e-learning o de su sistema de notificaciones automáticas.

Análisis del enlace:

URL observada:

https://elearning.trabajo.gob.ec/login/forgot_password.php

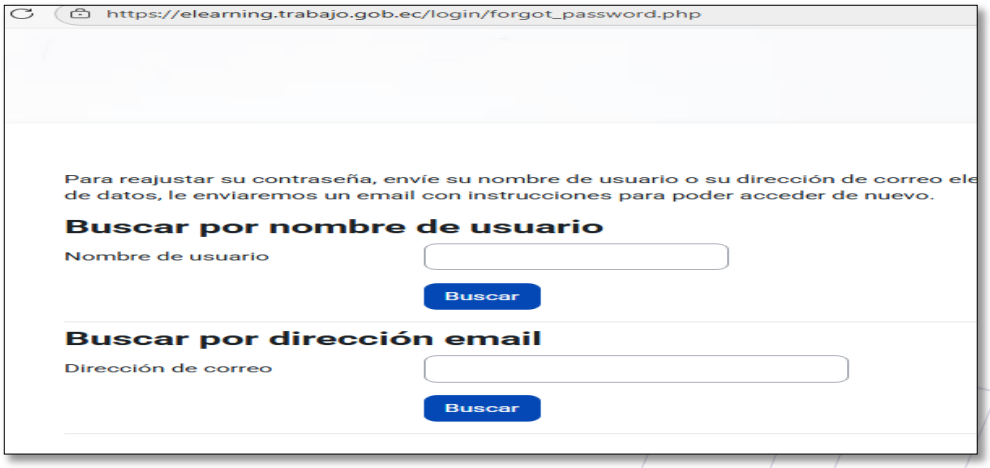

Figura 1. Evidencia del enlace malicioso en plataforma e-learning

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:	AL-2026-014	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **Aviso de seguridad**	ecucert
TLP:	TLP:CLEAR		
Fecha:	23-mar-2026	**Abuso de plataforma elearning.trabajo.gob.ec para envío de SPAM**	V 1.1

Durante el análisis se determinó que:

- El enlace redirige a la plataforma institucional de e-learning.
- Permite solicitar el cambio de contraseña mediante un mecanismo potencialmente débil.
- Durante la navegación se generan múltiples solicitudes HTTP/HTTPS hacia servicios externos.
- Se detectó la creación de un archivo temporal en el endpoint del usuario.

Conexiones externas observadas:

- ocsp.digicert.com
- ocsp.microsoft.com
- clients2.google.com
- cdn.jsdelivr.net

Este comportamiento sugiere que no se trata de un sitio de phishing externo, sino de un posible:

- Abuso del mecanismo de recuperación de contraseña
- Envío masivo de notificaciones automáticas (email flooding)
- Vulnerabilidad o compromiso parcial de la plataforma elearning.trabajo.gob.ec

IV. INDICADORES DE COMPROMISO:

Tipo	Indicador
Cuenta involucrada	noreply_elearning@trabajo.gob.ec
IP origen	190.152.44.225
Hostname	spf24.trabajo.gob.ec
URL observada	hXXps[:]//elearning[.]trabajo[.]gob[.]ec/login/change_password.php
Hash	cdb4ee2aea69cc6a83331bbe96dc2caa9a299d21329efb0336fc02a82e1839a8

Tabla 1. IOCs involucrados

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:	AL-2026-014	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **Aviso de seguridad**	ecucert
TLP:	TLP:CLEAR		
Fecha:	23-mar-2026	**Abuso de plataforma elearning.trabajo.gob.ec para envío de SPAM**	V 1.1

V. RECOMENDACIONES:

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

- Coordinar con el equipo del Ministerio del Trabajo la revisión de seguridad de la plataforma elearning.trabajo.gob.ec.
- Verificar posibles abusos del mecanismo de recuperación de contraseña y notificaciones automáticas.
- Revisar logs de autenticación, servidor web (Apache/Nginx) y servidor SMTP asociados al host spf24.trabajo.gob.ec.
- Evaluar la integridad del sistema LMS (plugins, scripts y configuraciones).
- Implementar controles adicionales como:
  - Rate limiting
  - CAPTCHA
  - Autenticación multifactor (MFA)

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