

RESTRICCIÓN DE ACTIVIDADES DE ESCANEOS Y PRUEBAS DE SEGURIDAD SOBRE INFRAESTRUCTURA SET-FX

Estimados afiliados,

Con el fin de proteger la disponibilidad, integridad y continuidad de los sistemas e información que soportan la operación de SET-FX, y en coherencia con nuestro Sistema de Gestión de Seguridad de la Información y Ciberseguridad, nos permitimos informar y reiterar lo siguiente.

SET-FX gestiona la ciberseguridad y la seguridad de la información conforme al marco regulatorio aplicable de la Superintendencia Financiera de Colombia (SFC) y bajo lineamientos de referencia y buenas prácticas reconocidas. En virtud de lo anterior, contamos con controles internos y mecanismos formales para la identificación, evaluación y tratamiento de vulnerabilidades, así como actividades de verificación y aseguramiento de seguridad ejecutadas bajo un modelo controlado, con alcance, ventanas de ejecución y responsables definidos.

Por lo anterior, queda expresamente prohibida la ejecución, por parte de afiliados y/o terceros actuando en su nombre, de cualquier actividad técnica de evaluación ofensiva o pruebas de seguridad sobre la infraestructura tecnológica de **SET-FX**.

Esta prohibición incluye, de manera enunciativa y no limitativa:

- Escaneos o “pruebas” de vulnerabilidades (automáticas o manuales).
- Pruebas de penetración (pentesting), explotación de debilidades o intentos de intrusión.
- Actividades de “ethical hacking”, red teaming, simulaciones de ataque, fuzzing o pruebas técnicas con fines de seguridad.
- Reconocimiento y enumeración de servicios, análisis de puertos, validación de credenciales, fuerza bruta u otras acciones similares.
- Cualquier interacción no autorizada con los sistemas de comunicación establecidos, APIs, servicios o componentes adicionales asociados al sistema SET-FX.

Aun cuando se realicen con intención de verificación, estas actividades pueden afectar la continuidad del servicio, interferir con mecanismos de monitoreo y respuesta, generar eventos de seguridad o alertas operativas, falsos positivos e incrementar el riesgo operacional.

La presente directriz aplica a toda la infraestructura de SET-FX, incluyendo, servidores, redes, plataformas, aplicación e interfaces.



SET-FX valora el enfoque responsable frente a la seguridad. Si el afiliado necesita soportes para sus auditorías o debida diligencia, por favor enviar la solicitud a comercial@set-icap.co y se entregará una certificación/constancia que respalde que SET-FX realiza internamente ejercicios de seguridad y gestión de vulnerabilidades.

El incumplimiento de esta directriz podrá derivar en medidas previstas en los acuerdos aplicables, incluyendo —según corresponda— restricciones de acceso, bloqueo de la aplicación en la activación de protocolos de seguridad y demás acciones contractuales y/o legales a que haya lugar.

Finalmente, si algún afiliado identifica un potencial riesgo o vulnerabilidad relacionada con SET-FX, deberá reportarlo al canal Tecnologia@set-icap.co evitando ejecutar pruebas intrusivas. SET-FX evaluará el reporte y gestionará las acciones correspondientes.

Agradecemos su atención y cumplimiento. Esta medida busca proteger la estabilidad del sistema y la continuidad de la operación.

Atentamente,



FRANZ CHAMORRO
Gerente TI