CERTIFICACIÓN CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

SET-ICAP FX, identificada con NIT **830.115.054-3** con licencia otorgada por la Superintendencia Financiera de Colombia (SFC) y, en su calidad de **proveedor de infraestructura** para el mercado financiero, certifica a quien corresponda que:

1. Propósito de esta certificación

La presente certificación se emite y publica como respuesta institucional a solicitudes de Afiliados al sistema SET-FX, proveedores y terceros relacionadas con nuestras prácticas, controles y actividades en materia de ciberseguridad y seguridad de la información, incluyendo —de manera enunciativa y no limitativa— requerimientos de debida diligencia, evaluaciones de proveedores, solicitudes de aseguramiento y requerimientos de información sobre controles de seguridad.

2. Marco regulatorio y de referencia

SET-ICAP mantiene un marco de gestión soportado en lineamientos y buenas prácticas aplicables, que incluye, según corresponda al alcance:

- **Superintendencia Financiera de Colombia (SFC):** Circular Básica Jurídica (C.E. 029 de 2014) y sus modificaciones, incluyendo lo establecido en la Circular Externa 007 de junio de 2018, mediante la cual se definen requisitos mínimos para la gestión de riesgos asociados a ciberseguridad **y** seguridad de la información, así como demás disposiciones aplicables.
- **Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC):** alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI) y sus guías vigentes, en lo pertinente.
- **Estándares y buenas prácticas internacionales** (referenciales): marcos y estándares reconocidos de gestión de seguridad y riesgos, tales como ISO/IEC 27001 (sistemas de gestión) e ISO/IEC 27002 (controles), y/o marcos equivalentes, cuando aplique.

3. Declaración de prácticas, actividades y controles

SET-ICAP cuenta con un Sistema/Programa de Gestión de Seguridad de la Información y Ciberseguridad, basado en gestión de riesgos y mejora continua, orientado a preservar la confidencialidad, integridad, disponibilidad y trazabilidad de la información y de los activos tecnológicos que soportan su operación. De manera general, dicho sistema incorpora las siguientes prácticas y actividades:

Gobierno, riesgo y cumplimiento

- Gobierno de seguridad con roles y responsabilidades definidos, políticas, procedimientos y lineamientos de operación.
- Gestión de riesgos de seguridad aplicada a procesos y activos críticos (identificación, valoración, tratamiento y seguimiento.
- Seguimiento al cumplimiento de lineamientos regulatorios aplicables, en lo pertinente al alcance.

Gestión de activos, información y trazabilidad

- Inventario y administración de activos relevantes, con criterios de criticidad y lineamientos de clasificación y manejo de información.
- Controles de trazabilidad y registro (logging) de actividades relevantes, conforme a necesidades operativas y de auditoría.
- Lineamientos de retención y disposición segura de información, según políticas internas y requerimientos aplicables.

Gestión de identidad, accesos y privilegios

- Controles de autenticación y autorización para usuarios internos y externos autorizados, bajo principios de mínimo privilegio.
- Administración del ciclo de vida de accesos (activaciones, modificaciones e inactivaciones), revisiones periódicas y controles reforzados para cuentas privilegiadas.
- Segregación de funciones cuando aplique, para reducir riesgos operativos y de seguridad.

Seguridad en el desarrollo y ciclo de vida de software (SSDLC)

- Implementación de prácticas de desarrollo seguro para aplicaciones y componentes propios, integrando consideraciones de seguridad.
- Segregación de ambientes, con controles para evitar cambios no autorizados y reducir riesgos operativos y de seguridad.
- Controles de gestión de cambios y liberaciones para software y componentes críticos (aprobaciones, validaciones, registro y trazabilidad).
- Lineamientos para el manejo seguro de configuraciones y dependencias, control de acceso a repositorios y herramientas de desarrollo, acorde con roles y responsabilidades.

Protección de infraestructura, hardening, segregación y seguridad técnica

- Configuración segura (hardening) y controles de protección para componentes tecnológicos, acorde con criticidad y buenas prácticas.
- Controles de segmentación y protección perimetral y/o interna, acordes con el modelo de operación.
- Segregación lógica y operativa de entornos y componentes críticos, de acuerdo con el diseño de la operación y la necesidad de reducir el riesgo.

- Gestión de cambios para componentes críticos, con controles de autorización, registro, trazabilidad y validación del cambio.

Gestión de vulnerabilidades y parches

- Identificación, priorización y remediación de vulnerabilidades basada en criticidad y exposición, con seguimiento y verificación de cierre.
- Gestión de parches y actualizaciones, ventanas operativas.

Monitoreo, detección y respuesta (SOC / SIEM)

- Operación de capacidades de monitoreo y análisis de eventos de seguridad mediante **SOC** y herramientas de correlación y detección, incluyendo **SIEM**, orientadas a identificar anomalías, amenazas y eventos.
- Gestión de eventos e incidentes con procedimientos de identificación, análisis, contención, erradicación, recuperación y lecciones aprendidas, con escalamiento interno según criticidad.

Continuidad, respaldos y resiliencia

- Respaldo de información y mecanismos de continuidad/recuperaciones acordes con la criticidad de los servicios y activos tecnológicos.
- Pruebas o verificaciones de recuperación.

Infraestructura, datacenters y controles físicos/lógicos

- Operación de infraestructura alojada en datacenters, con controles de seguridad física y lógica acordes con la criticidad, y medidas para preservar la disponibilidad del servicio.

Gestión de terceros y cadena de suministro

- Evaluación y gestión de riesgos de seguridad de proveedores y terceros críticos, con controles contractuales (confidencialidad, manejo de información, requisitos de seguridad) y seguimientos periódicos.

Concientización, auditoría y mejora continua

- Programas de sensibilización y formación en seguridad para colaboradores, con enfoque por roles cuando aplique.
- Revisiones internas y/o auditorías (según aplique), seguimiento a hallazgos, planes de acción y verificación de efectividad de controles.

4. Confidencialidad y limitaciones

- Esta certificación tiene carácter informativo y no divulga información sensible o confidencial.
- La seguridad se gestiona bajo un enfoque basado en riesgos; por tanto, este documento no constituye garantía absoluta de ausencia de vulnerabilidades o

incidentes, sino evidencia de la implementación de un sistema de gestión y controles bajo un modelo de mejora continua.

5. Vigencia

La presente certificación se emite con fecha 25 de febrero de 2026 y tiene vigencia hasta que sea actualizada por cambios regulatorios, ajustes relevantes en el alcance o actualizaciones del marco interno de seguridad.

Firmado por:

Franz Chamorro
Gerente TI