60 AÑOS

asobanca
Asociación de Bancos del Ecuador

LAW JOURNAL

OCTUBRE 2025

EDICIÓN ESPECIAL

VII Jornadas de Seguridad Bancaria

PUBLICADO EN OCTUBRE DE 2025

Elaborado por el Departamento Legal de ASOBANCA

Director Ejecutivo
Dr. Marco Antonio Rodríguez

Directora Legal
Dra. María Gabriela López

Asesor Legal
Abg. Jhossueth Almeida

Asesor Legal
Abg. Víctor Obando

Asesora Legal Jr.
Abg. María Cristina Castellanos

Asesor Legal Jr.
Abg. Henry Narváez

Asistente Legal
Mateo Andrade

Av. República de El Salvador N25-204 y Suecia.
Edificio Delta 890 - Piso 7.

TELÉFONO

(593-2) 2466 700
www.asobanca.org.ec

TABLA DE CONTENIDO

EDITORIAL

Seguridad bancaria del futuro: La convergencia de lo físico y lo digital

Los últimos quince años han marcado un periodo de profunda transformación para el sector financiero privado, especialmente en el ámbito digital, impulsando cambios estructurales que van desde la reorganización interna de las instituciones hasta la manera en que los clientes interactúan con los servicios y productos financieros. La digitalización no solo transformó los canales de atención, sino también la concepción misma de la seguridad en el sistema financiero, que pasó de un enfoque centrado en lo físico hacia un modelo de gestión integral de riesgos físicos y digitales.

A finales de la primera década de este siglo, las instituciones financieras concentraban sus esfuerzos en fortalecer la seguridad de instrumentos físicos que permitían realizar transacciones de forma masiva, como el cheque. Los departamentos legales de las entidades financieras debatían los mejores mecanismos para mejorar las seguridades del cheque y reducir los tiempos de efectivización del mismo. Uno de los principales avances fue lograr que la compensación y acreditación de los cheques se realice en un plazo máximo de 24 horas, aunque siempre sujeta al documento físico.

Hoy, ese escenario parece lejano, y algunas de las prácticas de entonces, resultan difíciles de imaginar en la dinámica digital actual. Las instituciones financieras han pasado de procesar operaciones interbancarias en cortes horarios definidos a implementar mecanismos de acreditación inmediata, donde una transferencia puede pasar de una cuenta a otra en segundos.

El advenimiento de nuevas tecnologías ha abierto un espacio sin precedentes para mejorar la eficiencia, accesibilidad y experiencia de los usuarios, pero también ha planteado nuevos retos: proteger su información, garantizar la autenticidad de las transacciones y preservar la confianza del cliente en entornos cada vez más interconectados. La seguridad se ha convertido en uno de los ejes sobre los cuales se sostiene la estabilidad y buena reputación del sistema financiero; y este es el resultado de un equilibrio adecuado entre innovación y seguridad.

El estudio de Asobanca *"La resiliencia de la banca digital ante entornos desafiantes"* reveló que en 2024 el 67,7% del total de transacciones se realizaron por canales digitales, consolidando un cambio estructural en la forma en que los ecuatorianos interactúan con sus entidades financieras de preferencia. Detrás de esa cifra existe un esfuerzo continuo de las instituciones por fortalecer su infraestructura tecnológica, mejorar sus capacidades de respuesta ante incidentes y elevar los estándares de ciberseguridad.

Los teléfonos inteligentes introdujeron un hito en los mecanismos de autenticación del usuario mediante la validación biométrica, permitiendo identificar a las personas a través de su huella o incluso de su rostro, algo que hace pocos años parecía difícil de imaginar. Sin duda, la evolución tecnológica ha impulsado la innovación de los servicios financieros y ha mejorado significativamente la experiencia del usuario, sin embargo, esa misma evolución se ha convertido también en un aliado para los actores maliciosos: la autenticación biométrica, considerada hasta hace poco como una de las capas más seguras de verificación, hoy enfrenta nuevos riesgos derivados de la inteligencia artificial y la manipulación de imágenes o voces, capaces de comprometer incluso los sistemas más avanzados de identificación.

Los dispositivos móviles también se han convertido en un nuevo frente de riesgo. A través de mecanismos como el SIM *swapping,* el *smishing,* el *spoofing* o el *vishing,* los delincuentes buscan vulnerar la identidad digital de los usuarios y acceder a sus cuentas o datos personales, aprovechándose de la confianza del usuario en las entidades financieras y brindándoles acceso a información sensible. Estas modalidades evidencian que, a medida que la tecnología avanza, también lo hacen las amenazas, lo que exige fortalecer la prevención, la educación digital y la cooperación entre todos los actores del sistema financiero e inclusive sectores como telecomunicaciones.

Ante escenarios cada vez más cambiantes y en constante evolución, los bancos han intensificado su trabajo para fortalecer la seguridad de los canales electrónicos, conscientes de que son hoy el medio más utilizado por los usuarios financieros. No obstante, la seguridad física de las entidades, sus instalaciones y clientes continúa siendo tan prioritaria como la ciberseguridad y la prevención de fraudes.

La convergencia de ambos ámbitos ha dado lugar al concepto de *seguridad integral* o *ciberfísica,* que reconoce la interdependencia entre la protección tecnológica y la protección del entorno físico. Bajo esta visión, la seguridad deja de ser un conjunto de acciones aisladas para convertirse en una estrategia coordinada que abarca desde la infraestructura tecnológica y los sistemas de vigilancia, hasta los protocolos de respuesta y la capacitación del personal. Precisamente, este enfoque es el eje central de las VII Jornadas de Seguridad Bancaria, un espacio para analizar los nuevos riesgos que enfrenta el sistema financiero y compartir experiencias que fortalezcan la resiliencia colectiva del sector.

La presente edición especial de Law Journal con motivo de las VII Jornadas de Seguridad Bancaria, organizadas por la Asociación de Bancos Privados del Ecuador – ASOBANCA - y su Comité Ecuatoriano de Seguridad Bancaria Integral presentan una reflexión amplia sobre la seguridad bancaria entendida como un desafío integral, donde convergen la tecnología, la gestión del riesgo y el marco regulatorio. Desde distintas perspectivas, los artículos destacan cómo la innovación y la protección deben avanzar de la mano para garantizar la confianza en un entorno cada vez más digitalizado. La seguridad, en términos generales, guarda una estrecha conexión con aspectos legales que resultan esenciales para el buen funcionamiento y confianza del sistema financiero. La normativa aplicable a las entidades en materia de riesgos operativos y tecnológicos se consolida como un pilar estratégico para preservar la estabilidad, la continuidad de las operaciones y la confianza de los usuarios en la banca.

Construyendo confianza: El compromiso de los bancos con la seguridad digital

Laura Ureta
Oficial de Seguridad de la Información de Banco Bolivariano

En la era digital, la confianza es un activo invaluable para las instituciones financieras. Los bancos deben proteger la información sensible de sus clientes y garantizar la integridad de sus sistemas para mantener la confianza y evitar pérdidas significativas. La promesa de la banca digital (conveniencia, velocidad y accesibilidad) solo se materializa si se cimenta en una seguridad inquebrantable. La seguridad digital ya no es solo una función de soporte técnico, sino un pilar estratégico y un diferenciador competitivo crucial que define la relación entre un banco y sus clientes.

La digitalización ha transformado la forma en que los bancos interactúan con sus clientes. La banca en línea, las aplicaciones móviles y los pagos digitales han mejorado la conveniencia y la eficiencia, pero también han aumentado el riesgo de ciberataques y filtraciones de datos. Los bancos deben adaptarse a este nuevo entorno y priorizar la seguridad digital para proteger sus activos y la confianza de sus clientes.

El surgimiento de la banca digital y, más recientemente, el auge de las Fintech impulsó una migración masiva de servicios a plataformas en línea y móviles. Esta transformación, acelerada por la pandemia de COVID-19 en Latinoamérica, significó un enorme beneficio en términos de inclusión financiera y eficiencia operativa. Sin embargo, este nuevo ecosistema digital también amplió la superficie de ataque de manera exponencial.

Históricamente, los bancos se enfocaban en la seguridad perimetral (firewalls y sistemas de detección de intrusiones). Hoy, el enfoque ha cambiado a la seguridad centrada en los datos y la resiliencia operativa. Los atacantes actuales emplean tácticas sofisticadas como el ransomware, el phishing dirigido (a empleados y clientes), el compromiso de credenciales privilegiadas, y la explotación de vulnerabilidades en las APIs (Interfaces de Programación de Aplicaciones), que son la columna vertebral de la banca moderna. En Latinoamérica, el malware y las campañas de phishing son incidentes comunes, lo que subraya la necesidad de una postura de seguridad proactiva y orientada a la confianza del usuario.

¿Qué implica la Confianza Digital?

La confianza digital se refiere a la percepción que tienen los clientes de que sus datos y transacciones estén seguros y protegidos por el Banco, esto se traduce en la capacidad de una institución para proteger sus datos, garantizar la privacidad de sus interacciones y asegurar la disponibilidad de sus servicios, incluso frente a ciberataques.

La confianza digital, implica no solo la implementación de medidas de seguridad efectiva, sino también la transparencia y la comunicación clara con los clientes sobre los riesgos y las medidas de seguridad.

Implica cuatro pilares fundamentales:

1. **Seguridad de los Datos:** El banco debe asegurar la confidencialidad, integridad y disponibilidad (CID) de toda la información. Esto significa utilizar cifrado robusto para datos en tránsito y en reposo, implementar la tokenización para reducir la exposición de información sensible y aplicar controles de acceso estrictos.

2. **Privacidad y Transparencia:** El cliente debe tener la seguridad de que su información personal no solo está protegida de ataques externos, sino que también es gestionada de forma ética, transparente y conforme a las regulaciones de protección de datos.

3. **Resiliencia Operacional:** La capacidad del banco para mantener sus servicios operativos de manera continua, a pesar de fallas técnicas, desastres naturales o ciberataques. Los clientes confían en que podrán acceder a su dinero 24/7.

4. **Experiencia del Usuario Segura:** La seguridad no debe ser un obstáculo, implementar mecanismos como la autenticación multifactor (MFA) de manera sencilla y transparente, y ofrecer herramientas de seguridad intuitivas (como notificaciones de transacciones en tiempo real) refuerza la confianza.

Reconocer la importancia de construir confianza, es esencial para mantener una relación sólida entre el banco y el cliente, sobre todo para tener éxito en el panorama financiero actual, lo cual se traduce en que los clientes:

1. **Permanezcan leales:** confían en su banco tienen mayor probabilidad de permanecer en el a largo plazo

2. **Recomienden el banco:** satisfechos y confiados pueden recomendar el banco a amigos y familiares, así como potenciar sus experiencias

3. **Utilicen más servicios:** confían en su banco y tienen mayor predisposición a utilizar más servicios y productos financieros.

Desafíos y Riesgos de no abordar la confianza digital

Desafíos claves

Fomentar la confianza de los clientes, sin lugar a duda es una prioridad para los bancos, los diversos retos que enfrentamos pueden minar estos esfuerzos. Los bancos enfrentan varios desafíos en la implementación de medidas de seguridad digital efectivas. Algunos de los más significativos incluyen:

1. **La complejidad de los sistemas / sistemas legados:** Los sistemas bancarios son complejos y heterogéneos, lo que dificulta la implementación de medidas de seguridad uniformes. Muchos bancos tradicionales operan con infraestructuras antiguas que son difíciles y costosas de asegurar, actualizar y monitorear, creando vulnerabilidades persistentes.

2. **Crecimiento Exponencial de APIs y la Nube:** La migración a entornos multicloud y la arquitectura de microservicios basada en APIs aumenta la complejidad y el riesgo si no se implementan controles de seguridad API-first.

3. **La evolución de las amenazas:** Los ciberataques están en constante evolución, lo que requiere que los bancos estén siempre actualizados y adaptados a las nuevas amenazas.

4. **La regulación y el cumplimiento:** Los bancos deben cumplir con una variedad de regulaciones y normas de seguridad, lo que puede ser un desafío significativo.

5. **La conciencia y la educación:** El eslabón más débil sigue siendo el humano. La falta de personal de ciberseguridad especializado en Latinoamérica y la necesidad de una capacitación continua y efectiva para toda la plantilla y los clientes son desafíos persistentes. Los trabajadores y los clientes deben estar conscientes de los riesgos de seguridad y saber cómo protegerse.

Riesgos de no abordar la confianza digital

Si los bancos no abordan la confianza digital de manera efectiva, pueden enfrentar varios riesgos, incluyendo:

1. **Pérdida de clientes:** Los clientes pueden perder la confianza en el Banco y cambiarse a un competidor.

2. **Daño a la reputación:** Éxodo de clientes, pérdida de nuevos clientes y críticas negativas en medios y redes sociales. Los incidentes de seguridad pueden dañar la reputación del Banco y afectar su imagen pública.

3. **Pérdidas financieras:** Fraude, robo de fondos, costos de remediación post-incidente y multas regulatorias. Los incidentes de seguridad pueden resultar en pérdidas financieras para el banco y sus clientes.

4. **Litigios y Responsabilidad Civil:** Demandas colectivas por parte de clientes afectados por la filtración de datos.

5. **Paralización de Servicios (Downtime):** La interrupción de servicios críticos debido a un ataque (como un ataque de denegación de servicio, DDoS) erosiona de inmediato la confianza.

Estrategias para construir confianza

Para un banco, la confianza es el activo no financiero más importante. Su ausencia tiene repercusiones directas en la viabilidad del negocio. Para fortalecer su compromiso con la seguridad digital, los bancos pueden considerar las siguientes estrategias:

1. **Implementar una estrategia de seguridad integral:** Los bancos deben desarrollar una estrategia de seguridad que abarque todos los aspectos de la seguridad digital, desde la protección de la infraestructura hasta la educación de los trabajadores y clientes.

2. **Invertir en tecnologías de seguridad avanzadas:** Los bancos deben invertir en tecnologías de seguridad avanzadas, como la autenticación multifactor, el cifrado de los datos, la inteligencia artificial y el aprendizaje automático, para detectar y prevenir ciberataques.

3. **Fomentar la colaboración y el intercambio de información:** Los bancos deben colaborar con otros bancos, instituciones financieras y organismos reguladores para compartir información y mejores prácticas de seguridad.

4. **Priorizar la conciencia y la educación:** Los bancos deben priorizar la conciencia y la educación de los empleados y clientes sobre los riesgos de seguridad y cómo protegerse.

5. **Realizar pruebas y simulacros:** Los bancos deben realizar pruebas y simulacros de seguridad para identificar vulnerabilidades y mejorar su capacidad de respuesta ante incidentes.

Ejemplos Bancarios en Latinoamérica

Varios bancos en la región están demostrando su compromiso al adoptar estrategias avanzadas:

1. **Adopción de la IA en la Detección de Fraude (Brasil y México):** Grandes bancos en estos países utilizan algoritmos de Machine Learning para analizar millones de transacciones por segundo, identificando patrones anómalos de comportamiento que son invisibles para los sistemas de reglas tradicionales, lo que reduce el fraude en tiempo real.

2. **Implementación de Biometría y MFA (Colombia y Perú):** Bancos en la región han estandarizado el uso de biometría (huella dactilar, reconocimiento facial) para accesos y transacciones de alto valor, fortaleciendo la autenticación del cliente y haciendo la experiencia más cómoda.

3. **Transparencia en la Respuesta a Incidentes (Chile):** Algunas instituciones han mejorado sus protocolos de comunicación, informando rápidamente sobre intentos de ataque fallidos o vulnerabilidades detectadas (sin exponer detalles técnicos sensibles), lo cual demuestra control y madurez.

Cómo debe evolucionar el marco normativo en pro de la confianza digital

El marco normativo debe evolucionar para abordar los desafíos de la seguridad digital y proteger la confianza de los clientes. Algunas recomendaciones incluyen:

1. **Regulación de Resiliencia Operacional:** Las normativas deben exigir no solo la prevención, sino también la capacidad de recuperación y continuidad del negocio. Modelos como el Reglamento de Resiliencia Operacional Digital (DORA) de la Unión Europea deben servir de inspiración para establecer estándares mínimos de gestión de riesgos de TICs para entidades financieras y sus terceros proveedores críticos. Las regulaciones deben actualizarse para reflejar los cambios en el entorno digital y abordar los nuevos riesgos y desafíos.

2. **Regulación "API-First" y Open Banking:** A medida que el Open Banking se propaga, las regulaciones deben establecer pautas claras y estrictas para la seguridad de las APIs que gestionan el intercambio de datos de clientes con terceros, asegurando que la innovación no comprometa la seguridad.

3. **Mayor colaboración:** Los organismos reguladores deben colaborar con los bancos y otros actores para compartir información y mejores prácticas de seguridad.

4. **Educación y conciencia:** Los organismos reguladores deben promover la educación y la conciencia sobre los riesgos de seguridad y cómo protegerse.

Conclusiones

El compromiso de los bancos con la seguridad digital no es una opción, sino un imperativo moral y de negocio. La confianza digital se construye día a día, con cada transacción segura, cada dato protegido y cada comunicación transparente.

Los bancos latinoamericanos están en una encrucijada crítica: pueden elegir ver la seguridad como un centro de costos o como una inversión estratégica fundamental que garantiza su longevidad y relevancia en la economía digital. La evolución de la amenaza, el dinamismo del mercado Fintech y las crecientes exigencias regulatorias exigen una respuesta audaz.

La seguridad digital es un aspecto crítico para los bancos en la era digital. Al implementar medidas de seguridad efectivas y priorizar la conciencia y la educación, los bancos pueden proteger la confianza de sus clientes y evitar pérdidas significativas. Los bancos ecuatorianos están comprometidos con la seguridad digital y trabajan juntos para proteger la confianza y la integridad del sistema financiero.

La colaboración y el intercambio de información entre los bancos, los organismos reguladores y supervisores son fundamentales para abordar los desafíos de seguridad digital y construir un entorno financiero más seguro.

El futuro de la banca es digital, y su base es la confianza. Solo los bancos que integren la ciberseguridad en el núcleo de su estrategia, que inviertan en resiliencia avanzada y que logren transformar a sus clientes y trabajadores en aliados de la seguridad, serán los que logren construir esa confianza inquebrantable y prosperar en el siglo XXI.

Seguridad digital en la banca: Implicaciones y aportes para el fortalecimiento del Índice Global de Ciberseguridad en Ecuador

Fabián Íñiguez
Director de operaciones en Grupo RADICAL

Introducción

La seguridad digital en la banca se ha convertido en un pilar esencial para garantizar la confianza de los clientes, la estabilidad del sistema financiero y la competitividad del país en el ámbito internacional. En un entorno marcado por la acelerada digitalización de los servicios y el incremento de amenazas cibernéticas, el sector financiero ecuatoriano enfrenta el desafío de combinar innovación tecnológica con altos niveles de protección de la información y resiliencia operativa.

El Índice Global de Ciberseguridad (GCI), elaborado por la Unión Internacional de Telecomunicaciones (UIT), constituye el principal referente internacional para medir los compromisos de los Estados en esta materia. En el caso de Ecuador, el avance ha sido notable. Este progreso no responde únicamente a las disposiciones regulatorias de la Superintendencia de Bancos, sino también al liderazgo del sector financiero y de los Oficiales de Seguridad de la Información (CISO, por sus siglas en inglés), quienes han adoptado estándares internacionales, fortalecido la gestión del riesgo operativo y promovido la innovación en seguridad digital.

El objetivo de este artículo es analizar las implicaciones de la seguridad digital en la banca ecuatoriana y su aporte al fortalecimiento del GCI, destacando cómo la conjunción de marcos regulatorios, innovación tecnológica y cooperación público-privada posiciona al sector financiero como un actor estratégico en la construcción de resiliencia digital y en la futura Ley de Ciberseguridad.

Análisis del Contexto Ecuatoriano

En los últimos cuatro años, Ecuador ha recorrido un camino de transformación profunda en materia de ciberseguridad. En 2020, el país apenas alcanzaba un puntaje de 26,30 en el Índice Global de Ciberseguridad (GCI) de la Unión Internacional de Telecomunicaciones (UIT), lo que reflejaba la necesidad urgente de construir marcos regulatorios sólidos y fortalecer la capacidad institucional. Sin embargo, en la edición 2024, el puntaje ascendió a 87,18, ubicando al Ecuador en el *Tier 2 – Advancing* y marcando un salto cualitativo que no fue fruto del azar, sino de un trabajo conjunto y sostenido.

Como exsubsecretario de Gobierno Electrónico del Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL), tuve la oportunidad de acompañar este proceso, liderando iniciativas que articularon esfuerzos entre el Estado, la academia, el sector privado y, de manera muy especial, la banca.

La construcción de confianza digital no se dio únicamente desde la normativa, sino en la capacidad de los bancos de implementar controles avanzados, planes de continuidad del negocio y estándares internacionales.

El compromiso de los CISO y sus equipos de ciberseguridad permitió traducir las disposiciones regulatorias en prácticas efectivas, protegiendo tanto a los usuarios como a la infraestructura crítica.

La normativa emitida por la Superintendencia de Bancos, en particular la *Norma de Control para la Gestión del Riesgo Operativo,* reforzó este camino al establecer obligaciones claras: contar con un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001, implementar planes de continuidad del negocio bajo ISO 22301, y reportar incidentes de seguridad en plazos definidos. Estas disposiciones, sumadas a la Ley Orgánica de Protección de Datos Personales, consolidaron un marco regulatorio que alineó al Ecuador con las mejores prácticas internacionales en materia de gobernanza de la información.

El sector financiero, por su parte, complementó este marco con la adopción de estándares y buenas prácticas globales como NIST *Cybersecurity Framework,* PCI DSS, Basilea III y, más recientemente, el *Digital Operational Resilience Act* (DORA) como referencia para una estrategia integral de resiliencia digital. Este alineamiento ha elevado los niveles de confianza digital, garantizando seguridad en las transacciones financieras y fortaleciendo la reputación del país frente a organismos multilaterales y a los mercados internacionales.

En conjunto, estos avances muestran que cuando se alinean la visión gubernamental, el marco regulatorio y la capacidad de ejecución del sector financiero, los resultados son tangibles.

No obstante, la historia aún está en construcción; para que Ecuador logre posicionarse entre los países de referencia global en ciberseguridad será indispensable profundizar los esfuerzos estratégicos, mantener la cooperación intersectorial y reforzar la innovación tecnológica, permitiendo que la banca continúe desempeñando un rol central en la consolidación de la resiliencia digital del país.

El rol de la banca en la confianza digital

La banca ecuatoriana ha sido un actor protagonista en el proceso de fortalecimiento de la ciberseguridad. Más allá de cumplir con las disposiciones regulatorias, las entidades financieras han impulsado la creación de Centros de Operaciones de Seguridad (SOC), la implementación de herramientas de Digital Forensics and Incident Response (DFIR) y la incorporación de tecnologías avanzadas como la autenticación multifactor y la biometría.

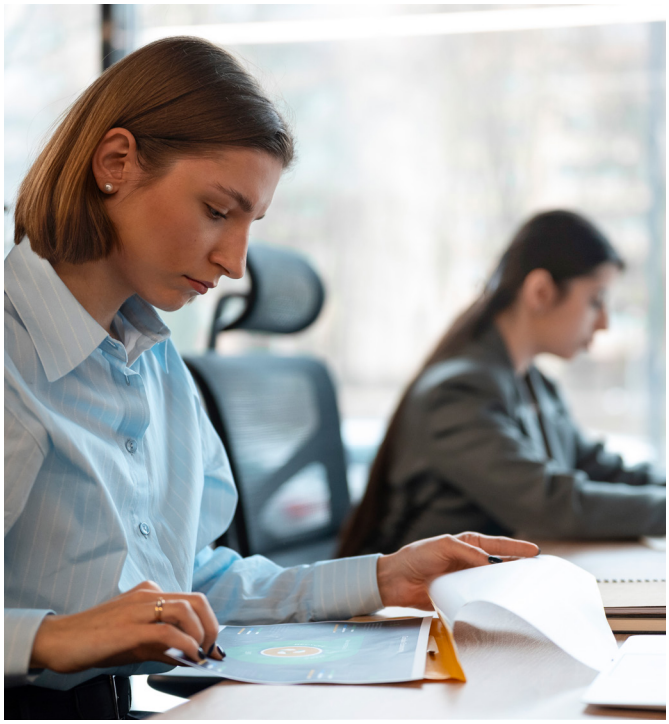
Asimismo, han robustecido sus planes de continuidad del negocio, alineándolos con estándares internacionales como ISO 22301. Estas iniciativas, lideradas por los CISO y sus equipos de ciberseguridad, han permitido mejorar la capacidad de respuesta frente a incidentes, elevar los niveles de resiliencia operativa y consolidar un entorno de mayor confianza tanto para los clientes como para las autoridades regulatorias.

Retos pendientes

No obstante, persisten desafíos relevantes. La brecha de talento especializado en ciberseguridad limita la sostenibilidad de los avances, y aún se requiere mayor frecuencia en los ejercicios nacionales de ciberresiliencia que evalúen la respuesta conjunta del sistema financiero y del Estado frente a amenazas críticas. Asimismo, la acelerada digitalización de los servicios bancarios amplía la superficie de ataque y exige cooperación público-privada en tiempo real para prevenir fraudes y mitigar riesgos.

Perspectiva estratégica

El camino hacia el *Tier 1 – Role Model* demanda que la banca continúe siendo un actor estratégico en la agenda nacional de ciberseguridad. Su participación activa en la construcción de la futura Ley de Ciberseguridad, junto con reguladores y legisladores, será fundamental para garantizar un marco jurídico moderno que equilibre innovación, seguridad y confianza digital. De esta manera, el sistema financiero no solo protege sus operaciones, sino que contribuye directamente a fortalecer la posición internacional del Ecuador en el GCI.



Conclusiones

El fortalecimiento de la seguridad digital en la banca es un elemento decisivo para consolidar la confianza en el sistema financiero y proyectar al Ecuador hacia un liderazgo regional en ciberseguridad. Los avances logrados en el Índice Global de Ciberseguridad (GCI) demuestran que el país cuenta con la capacidad de transformar marcos normativos y prácticas institucionales en resultados medibles, pero el camino hacia el Tier 1 – Role Model exige una visión estratégica de largo plazo.

La banca ecuatoriana, junto con los reguladores, tiene la oportunidad de convertirse en un agente de cambio y resiliencia digital, no solo cumpliendo disposiciones regulatorias, sino liderando la innovación, promoviendo la cooperación interinstitucional y contribuyendo de manera activa a la construcción de la Ley de Ciberseguridad que el país necesita. Este marco legislativo debe integrar estándares internacionales, inspirarse en estrategias de referencia como el DORA europeo y garantizar un equilibrio entre seguridad, innovación y competitividad.

De cara al futuro, resulta indispensable consolidar una agenda nacional de ciberseguridad financiera con cuatro ejes prioritarios:

1. **Talento humano:** formación de especialistas en ciberseguridad para reducir la brecha de capacidades.

2. **Ciberresiliencia:** fortalecimiento de los mecanismos de respuesta a incidentes mediante simulacros conjuntos y cooperación público-privada en tiempo real.

3. **Confianza digital:** promover la innovación tecnológica segura y concientización a los clientes en medios de pago, banca digital y servicios financieros inclusivos.

4. **Fomentar la innovación en ciberseguridad bancaria:** mediante el uso de inteligencia artificial, biometría avanzada, blockchain y analítica predictiva para la prevención de fraudes y la protección de las transacciones financieras.

En definitiva, la seguridad digital no debe ser vista únicamente como un requisito de cumplimiento, sino como un motor de competitividad y desarrollo sostenible. La banca ecuatoriana, como actor central en la economía, está llamada a desempeñar un rol protagónico en la construcción de un ecosistema digital resiliente, confiable y alineado con las mejores prácticas internacionales.

De la videovigilancia a la videointeligencia: ¿Cómo la banca redefine la seguridad e impulsa la experiencia del cliente en la nueva era digital?

José Marangunich R.

Gerente del Área de Seguridad Corporativa y Crimen Cibernético del Banco de Crédito BCP – CREDICORP

Lucero Alvarado N.

Gerente de Seguridad Ejecutiva, Investigaciones Corporativas, IA Aplicada & Analytics del Banco de Crédito BCP – CREDICORP

Revisando la última década respecto a los sistemas de videovigilancia en el ámbito de la seguridad bancaria en Latinoamérica, encontramos como punto común un enfoque predominantemente reactivo y muy orientado al forense, por lo cual podríamos definir que en la actualidad se cuenta con una orientación hacia tres frentes: la observación, el registro y el almacenamiento de evidencias. Este modelo clásico, impulsado principalmente en el cumplimiento de regulaciones en diferentes países, viene siendo objeto de un cambio no menor soportado principalmente en el uso de la inteligencia artificial generativa que viene teniendo desde el 2024 una creciente demanda para diversos usos.

En este contexto, podemos hablar de un cambio estratégico al movernos de un enfoque de la videovigilancia tradicional hacia un esquema de video inteligencia, caracterizado por el uso de analíticas avanzadas, información clave para el negocio y prospectiva de múltiples usos. Es así que, en un entorno donde los negocios, la tecnología y los riesgos avanzan raudamente y de manera disruptiva, la seguridad ha encontrado en la videointeligencia un aliado que acompaña este cambio que hoy impacta en todo tipo de industria, al contar con nuevas capacidades que abarcan tanto el campo táctico-operativo como el estratégico.

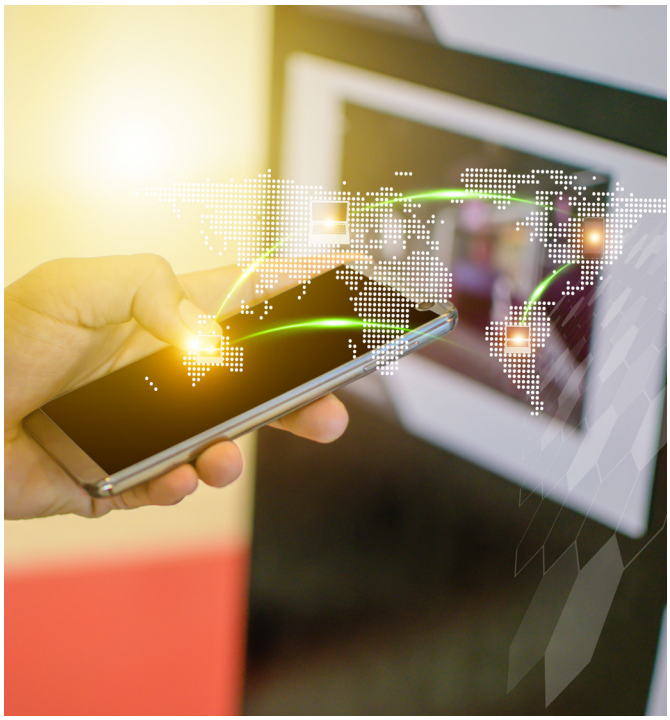
Hoy, la seguridad ya no puede limitarse a reaccionar ante incidentes o demanda de análisis forense como usualmente ocurría, por el contrario; se anticipa y genera información que la convierte en un habilitador clave para el negocio.

Es entonces que la actual mutación de una videovigilancia clásica a nuevas capacidades que nos trae la videointeligencia, resulta ser el punto de partida dentro del proceso de la transformación digital en la cual se encuentra inmersa un importante sector de la banca Latinoamericana.

La transformación: Tecnología, Negocios, Riesgos y Seguridad

La transformación digital viene revolucionando de manera acelerada la forma en que operan los negocios, la tecnología en que se soportan y los riesgos que deben gestionarse.

Este proceso ha impulsado un reenfoque de la seguridad, con múltiples aplicaciones que abarcan tanto en la experiencia al cliente, la gestión de infraestructura, el cumplimiento normativo, la gestión de personas y poder contar con un habilitador de información e inteligencia.



Este progreso ha traído consigo nuevos desafíos relacionados con la formación base para el empleo de esta nueva tecnología como el perfil de profesionales orientado principalmente en la formación de data y analytics.

En este contexto, la seguridad se ha posicionado como un eje transversal dentro de las organizaciones, integrando tecnología, procesos y talento para impulsar soluciones más eficientes, prospectivas y sostenibles.

Es importante citar, a manera de ejemplo, el caso de la banca peruana, donde la adopción de la videointeligencia se ha visto impulsada por tres factores determinantes:

1. El avance tecnológico, soportando un creciente negocio digital.

2. El marco regulatorio, definido por la Ley N° 30120, que autorizó la videovigilancia con fines de seguridad ciudadana, promulgada en 2013, y su reglamento publicado en 2020. Durante ese periodo, las instituciones financieras asumieron un rol activo de autorregulación, madurando procesos y fortaleciendo sus estándares internos hasta alcanzar niveles de cumplimiento y control más exigentes.

3. El contexto social, marcado por una percepción de inseguridad cada vez más alta en el Perú. De acuerdo con estudios de Datum, el 94% de los peruanos siente que la inseguridad ciudadana es un problema creciente, lo que refleja un entorno que demanda mayor protección para las personas, la infraestructura y la información. Es ahí, donde la videointeligencia cubre estas nuevas variables en los cuales se soporta el alcance de los nuevos modelos de seguridad.

Ante este escenario, la transformación se convirtió en un impulso para mirar más allá de las fronteras y buscar nuevas formas de fortalecer la seguridad, mejorar la eficiencia operativa y ofrecer una mejor experiencia a los clientes, tal como lo iremos comentando en el presente artículo y tomando como ejemplo el caso de la banca peruana.

Explorando nuevas latitudes

La necesidad de ampliar la visión estratégica de la seguridad producto de una nueva regulación en países como el Perú, llevó a observar de cerca lo que ya venían desarrollando otros mercados. Es en esa exploración que se identificaron que en distintos países de Asia y Europa, la videointeligencia formaba parte de ecosistemas tecnológicos consolidados, donde la analítica de datos, la automatización y la inteligencia artificial habrían transformado la manera como la seguridad se volvió un aliado del negocio teniendo directa presencia en la prevención de riesgos y mejora de la experiencia del cliente.

Estas referencias internacionales demostraron que el verdadero valor de la tecnología surge cuando se combina con una visión estratégica, un uso responsable de la información y equipos preparados para aprovechar su potencial. A partir de ese aprendizaje, se trazó una hoja de ruta enfocada en integrar soluciones avanzadas, desarrollar equipos y talento con mentalidad principalmente analítica y estratégica.

Cambiar el mindset es esencial, comprender que la seguridad moderna se construye con tecnología, pero se sostiene con talento que interpreta, actúa y evoluciona junto con ella.

Una nueva forma de generar valor

El desarrollo de la videointeligencia marcó una nueva etapa en la generación de valor como lo muestra la experiencia en el Perú a través de proyectos dirigidos por el banco líder. Este avance fortaleció tanto las capacidades internas como las externas, integrando tecnología en tiempo récord, formando talento especializado, además de lograr sinergias y colaboración estratégica con el propósito de construir un ecosistema de seguridad inteligente, conectado al negocio e incorporando valores como el cliente céntrico.

En el ámbito interno, el desarrollo de capacidades fue decisivo para consolidar una seguridad más ágil, analítica y alineada con los objetivos corporativos.

Las soluciones implementadas optimizaron la seguridad física, la salud ocupacional, la eficiencia operativa en los almacenes y la experiencia del cliente en las agencias. Cada una de estas dimensiones incorpora prácticas predictivas y automatización, reduciendo tiempos de respuesta y transformando la información en conocimiento para la toma de decisiones.

En el frente externo, lograr la cooperación en el ámbito gremial, las autoridades locales y las fuerzas a cargo del control de orden interno generó un modelo de seguridad colaborativo. Este modelo integra información de manera ética y responsable conforme a los marcos regulatorios con el fin de reforzar la protección de las personas, sus activos y la infraestructura.

Las capacidades desarrolladas siguen impulsando la evolución del modelo de videointeligencia. Integrar analítica avanzada, inteligencia artificial y colaboración interinstitucional optimizó procesos y potenció el talento que los lidera. Hoy, las capacidades técnicas y estratégicas del equipo son el eje que sostiene la anticipación, la agilidad y la eficiencia como pilares del valor.

Caso de Negocio soportado en Eficiencia, Alcance y Seguridad de la Información

El modelo se implementó sobre tres ejes fundamentales que, juntos logran un real caso de negocio bajo los lineamientos de eficiencia, alcance y seguridad de la información.

La eficiencia se traduce en procesos automatizados, reducción de costos, decisiones oportunas y un uso óptimo de los recursos. El alcance amplía la capacidad de la seguridad para integrarse con otras áreas del negocio y conectar personas, tecnología y propósito común. Y la seguridad de la información asegura un tratamiento ético, trazable y conforme a los marcos normativos, protegiendo la confianza de los clientes y la reputación institucional.

¿Por qué ir a la videointeligencia?

Como primera reflexión tenemos que su impacto trasciende lo tecnológico. Su verdadero valor surge de la combinación entre innovación, datos y talento especializado. Profesionales actualizados en analítica avanzada, inteligencia artificial y modelos predictivos garantizan que la inversión tecnológica se traduzca en conocimiento, prevención y confianza.

La seguridad inteligente representa la convergencia entre proteger y evolucionar, entre anticipar y generar valor. En un entorno donde la tecnología y los negocios avanzan con rapidez, el desafío no es alcanzar el ritmo: es liderarlo.

Cada día se ve con gran expectativa que las instituciones financieras de Latinoamérica están comprometidas en este proceso de transformación digital en el cual incorporan sí o sí la videointeligencia como una de sus principales propuestas de valor que buscan fortalecer sus capacidades, impulsar el conocimiento, promover una cultura de seguridad que inspire confianza, aprendizaje, experiencia e innovación sostenida. Es así que, a través de este artículo invitamos a los bancos e instituciones financieras de Latinoamérica y el Caribe para encontrar en la videointeligencia el aliado estratégico clave para nuestro tipo de negocio y que ya forma parte de un proceso de transformación digital cada día más disruptivo con la llegada de la inteligencia artificial generativa y próximamente con la superinteligencia artificial y la computación cuántica.

Responder con músculo: Cómo convertir planes de incidentes en acciones efectivas

Katherina Canales
Especialista en Ciberseguridad, fundadora y COO de Aura Cybersecurity

Hace unos años, durante mi gestión como directora operacional del CSIRT del Gobierno de Chile, aprendí una lección que hoy repito en cada charla y taller: no hay plan de respuesta ante incidentes que valga si no está pensado para operar en la realidad concreta de la organización. En papel, los protocolos pueden lucir impecables; en la práctica, cuando suena la alarma y la presión sube, la diferencia entre recuperarse con agilidad o protagonizar un espectáculo bochornoso es que el plan haya sido diseñado para personas, roles y procesos reales, y que haya sido probado en condiciones que simulen la tensión y el desorden que traen los incidentes complejos.

El primer error frecuente es asumir que la respuesta ante incidentes es solo un asunto técnico. Por supuesto que el diagnóstico forense, el *containment*, el *eradication* y la remediación técnica son el núcleo de la operación; pero cuando un incidente pase de ser un problema de TI a un hecho público con impacto en clientes, reguladores y operaciones críticas, la respuesta se convierte en un ejercicio multidisciplinario: equipo de TI, comunicaciones, jurídico, comité de crisis, áreas de negocio y proveedores externos. Un plan que no incorpora desde el diseño estas interdependencias está condenado a fracasar en la práctica.

Pensar en la organización real implica mapear no solo los sistemas claves, sino también las personas que toman decisiones, sus capacidades y sus tiempos de reacción. ¿Quiénes son los decisores que pueden autorizar desconexiones de sistema o suspender servicios? ¿Cuál es el vínculo contractual con terceros que suministran soporte crítico? ¿Dónde están los puntos de escalamiento para temas legales y regulatorios? Las respuestas deben estar plasmadas en el plan con nombres, roles y sustituciones funcionales, no con términos genéricos que en la hora cero se traducen en confusión. Recuerdo un incidente multisectorial donde la demora en autorizar la comunicación pública costó horas de exposición mediática evitables; la organización tenía el procedimiento, pero no había definido quién tenía la potestad final para aprobar un comunicado bajo presión.

Otro pilar que suele pasarse por alto es la claridad comunicacional interna y externa. En situaciones de crisis la información fluye rápido y, muchas veces, desestructurada. Sin una estrategia de comunicaciones integrada al plan de respuesta, los equipos técnicos terminan ocupándose de mensajes públicos o de atender preguntas de clientes, lo que resta foco a la contención técnica. El rol del equipo de comunicaciones debe estar definido con antelación: quién redacta el primer holding statement, quién lo valida, qué canales se emplean y cómo coordinar respuestas con áreas regulatorias y legales para evitar contradicciones o filtraciones que compliquen la respuesta. En uno de los ejercicios que coordinamos, la falta de alineación entre comunicaciones y legal generó un borrador público que apuntaba a una causa técnica que aún no habíamos verificado; la consecuencia fue una corrección pública que minó la confianza de clientes y medios.

La inclusión de asesoría legal desde el minuto cero no es un lujo: es una necesidad operativa. Las decisiones técnicas —por ejemplo, la recolección y preservación de pruebas, la colaboración con autoridades o la notificación a clientes y reguladores— tienen implicancias legales y regulatorias que deben ser consideradas antes de actuar. Un ejemplo claro es la manipulación de evidencias: un técnico que quiera “arreglar rápido” un sistema puede borrar logs o modificar timestamps con consecuencias para una investigación posterior. Tener a abogados que conozcan las obligaciones regulatorias y las mejores prácticas forenses evita acciones que comprometan la respuesta y la trazabilidad de la investigación.

Para que un plan funcione en la práctica hay que convertirlo en operativo: procedimientos paso a paso, playbooks accionables, listas de verificación y, sobre todo, responsabilidades claras.

Un *playbook* bien diseñado debe responder a la pregunta: ¿qué hace cada actor en los primeros 60, 120 y 360 minutos desde la detección? Estas ventanas temporales ayudan a priorizar acciones críticas como aislamiento de activos, recolección de evidencias, comunicación inicial y a coordinar recursos. La idea no es sustituir el juicio experto, sino reducir la fricción inicial para que la organización gane tiempo y no tome decisiones apresuradas que compliquen la remediación.

Sin embargo, ni los mejores *playbooks* sirven si no se ejercitan. La ejecución de ejercicios —tabletops, simulaciones en vivo, *Red Team / Purple Team* y pruebas de recuperación— es el mecanismo que evita que los protocolos terminen en letra muerta. Cuando coordinamos ejercicios multisectoriales aprendimos que un ejercicio bien planteado descubre no solo fallas técnicas, sino también problemas contractuales y de comunicación entre organizaciones que creen compartir información pero, en la práctica, no tienen acuerdos ni canales habilitados.

Los ejercicios cumplen varias funciones: validan supuestos técnicos, revelan vacíos en la cadena de mando, ponen a prueba los tiempos de respuesta y exponen fallas en la coordinación con terceros. Es importante que el diseño del ejercicio refleje escenarios plausibles y relevantes para la organización.

No sirve simular un *ransomware* de escritorio si la verdadera amenaza es una filtración de datos de un proveedor crítico. Los escenarios deben alinearse con el perfil de riesgo y con los activos que, en caso de comprometerse, generarían mayor impacto. Además, los ejercicios deben involucrar a los roles no técnicos y a los proveedores externos, incluir al departamento legal, a comunicaciones y al proveedor de servicios gestionados en el mismo simulacro aporta realismo y permite validar tiempos y decisiones conjuntas.

La metodología posejercicio es tan crítica como el ejercicio mismo. Sin revisión estructurada y lecciones aprendidas que se traduzcan en cambios concretos en los planes, cada ejercicio es solo un ensayo anecdótico. Un informe *postmortem* debe priorizar hallazgos por impacto y probabilidad, asignar responsables para las correcciones y definir plazos claros. Implementar una mejora sin seguimiento es tan peligroso como no hacer nada: crea una falsa sensación de seguridad.

La coordinación con proveedores externos merece un capítulo propio. Muchas organizaciones subcontratan SOCs, servicios forenses o backups gestionados, pero confían que esos proveedores operarán automáticamente cuando ocurra un incidente. Esto puede ser cierto parcialmente; sin embargo, es esencial integrar contractual y operacionalmente a esos actores: definir SLAs específicos para incidentes, puntos de contacto dedicados, acceso preautorizado para acciones críticas y ejercicio conjunto para asegurar interoperabilidad. En una respuesta real, el proveedor que no tiene acceso, o cuya autorización tarda horas por procesos administrativos, puede convertirse en un cuello de botella insalvable.

Un aspecto cultural no técnico, pero determinante, es la gestión del ego y la comunicación bajo presión. En incidentes críticos aparecen tensiones entre equipos, acusaciones implícitas y la tentación de buscar responsables en vez de soluciones. El objetivo del plan debe ser facilitar la colaboración, no la crítica inmediata. Establecer reglas de interacción en crisis, por ejemplo, canales de comunicación definidos, un lenguaje común y una política de "no culpar durante la contención", ayuda a mantener el foco en la remediación. Aprendí que equipos que practican este enfoque durante ejercicios tienden a mantener la calma y a tomar decisiones más efectivas en situaciones reales.

Finalmente, la gobernanza y el compromiso ejecutivo son indispensables. Sin el patrocinio de la alta dirección, los recursos, la prioridad y los cambios organizacionales necesarios para mantener un plan operativo difícilmente se materializan. La alta dirección debe entender que invertir en ejercicios y en integración multidisciplinaria no es un costo sino una reducción del riesgo reputacional, legal y operativo. Presentar métricas de mejora tiempo medio de detección y respuesta, reducción de impactos en simulaciones, cumplimiento de SLAs con proveedores facilita justificar esos recursos.

Hoy, convertir planes en respuesta efectiva exige tres líneas de trabajo integradas.

Primero, diseñar planes realistas y operativos que identifiquen roles, decisiones y dependencias concretas. Segundo, asegurar la participación multidisciplinaria con responsabilidades claras y definidas. Tercero, ejercitar y aprender: poner a prueba los planes con ejercicios pertinentes, revisar y priorizar hallazgos, y cerrar brechas con seguimiento riguroso. Mi experiencia en respuesta a incidentes complejos muestra que las organizaciones que articularon estas tres líneas respondieron más rápido, comunicaron mejor y recuperaron su operación con menos impacto. En el mundo actual, donde la exposición y la velocidad cuentan, la diferencia entre un plan que decora estanterías y uno que protege a la organización está en hacerlo operativo y practicar hasta que la respuesta sea un músculo.

Ciberinteligencia de Amenazas: Anatomía de un Ciberataque

Juan Carlos Beltrán
Chief Technology Officer de SecureSoft

En la era digital, la ciberseguridad se ha convertido en un pilar fundamental para la supervivencia y el éxito de cualquier organización. La célebre frase de John Chambers, ex CEO de CISCO Systems, *"Hay dos tipos de empresas: las que han sido hackeadas y las que aún no saben que lo han sido"*, resuena con más fuerza que nunca.

Esta afirmación subraya una realidad ineludible: la cuestión no es si una organización será atacada, sino *cuándo.* Ante este panorama, la ciber-resiliencia, la capacidad de una organización para anticipar, resistir, recuperarse y adaptarse a los ciberataques, se vuelve crucial.

El Creciente Panorama de las Ciberamenazas en América Latina

América Latina se ha convertido en un objetivo cada vez más atractivo para los ciberdelincuentes. Las estadísticas del primer trimestre de 2025 muestran un incremento alarmante en los ciberataques en la región, con un aumento del 25% en comparación con el mismo período del año anterior. Semanalmente, se registran un promedio de 2,716 ataques en LATAM, siendo los sectores Gubernamental y Financiero los más vulnerables.

El ransomware, un tipo de malware que cifra los datos de una víctima y exige un rescate para restaurar el acceso, es una de las amenazas más prominentes. De hecho, el 40% de los ataques atendidos por el equipo de Respuesta a Incidentes de Securesoft (Cyber Incident Response Unit – CIRU) en LATAM han sido de este tipo.

Un dato preocupante es que, a pesar de los riesgos, muchas empresas aún no están preparadas para enfrentar estas amenazas. De las organizaciones que pagaron un rescate por sus datos, solo el 16% logró recuperar su información.

Esto evidencia la importancia de no solo reaccionar ante los ataques, sino de implementar una estrategia efectiva de recuperación y prevención.

La Anatomía de un Ciberataque: Un Viaje por sus Fases

Para comprender cómo protegerse eficazmente, es esencial conocer las fases de un ciberataque.

Si bien cada ataque es único, la mayoría sigue una estructura similar. A continuación, describimos las técnicas que el equipo CIRU de Securesoft ha podido identificar a partir de su experiencia al responder a casi ochenta incidentes de alto impacto en la Región.

1. Reconocimiento:

En esta fase inicial, el atacante recopila la mayor cantidad de información posible sobre su objetivo. Esto puede incluir desde detalles técnicos sobre la infraestructura de la red hasta información sobre los empleados. Las técnicas comunes en esta etapa son:

- **Escaneos de reconocimiento activo (T1595):** Los adversarios exploran la red de la víctima en busca de puertos abiertos, servicios vulnerables y otros puntos de entrada.
- **Búsqueda de información en sitios web de libre acceso (T1593):** Se examinan sitios web de la empresa, redes sociales y otros recursos públicos para obtener información sobre la organización y su personal.

- **Recopilación de información sobre los hosts de la víctima (T1592):** Se busca información específica sobre los sistemas informáticos de la víctima, como direcciones IP, nombres de dominio y sistemas operativos.

2. Acceso Inicial:

Una vez que el atacante ha reunido suficiente información, busca una forma de infiltrarse en la red de la víctima. Las tácticas más frecuentes para lograr el acceso inicial son:

- **Suplantación de identidad (phishing) (T1566):** Se envían correos electrónicos fraudulentos que parecen legítimos para engañar a los empleados y hacer que revelen sus credenciales o descarguen malware.
- **Explotación de una aplicación pública (T1190):** Se aprovechan las vulnerabilidades en aplicaciones web y otros servicios expuestos a Internet para obtener acceso a la red.
- **Uso de credenciales de cuentas existentes (T1078):** Los atacantes pueden obtener credenciales a través de filtraciones de datos o comprarlas en la dark web para acceder a la red como si fueran usuarios legítimos.

3. Distribución:

Una vez dentro de la red, el atacante necesita moverse lateralmente para encontrar activos valiosos y establecer una presencia persistente. Para ello, pueden:

- **Abusar de los intérpretes de comandos y scripts (T1059):** Utilizan herramientas como PowerShell o cmd para ejecutar comandos maliciosos en los sistemas comprometidos.
- **Crear una cuenta (T1136):** Establecen nuevas cuentas de usuario para mantener el acceso a la red incluso si la cuenta original es descubierta y deshabilitada.
- **Programar tareas (T1053):** Configuran tareas programadas para ejecutar código malicioso en momentos específicos, lo que les permite mantener la persistencia y evadir la detección.

4. Explotación:

En esta fase, el atacante busca escalar privilegios y obtener un mayor control sobre la red. Esto puede implicar:

- **Explotar vulnerabilidades de software (T1068):** Se aprovechan las fallas de seguridad en el software para obtener acceso a nivel de administrador y tomar el control total de los sistemas.
- **Abusar de las credenciales de una cuenta local (T1078.003):** Utilizan cuentas locales con privilegios elevados para moverse por la red y acceder a información confidencial.
- **Uso de material de autenticación alternativo (T1550):** Se emplean técnicas como “pass the hash” o “pass the ticket” para autenticarse en otros sistemas sin necesidad de conocer las contraseñas de los usuarios.

5. Instalación:

Para mantener el control a largo plazo, los atacantes instalan herramientas y malware en la red de la víctima. Esto puede incluir:

- **Técnicas de fuerza bruta (T1110):** Se utilizan programas automatizados para probar miles de combinaciones de contraseñas y acceder a cuentas protegidas.
- **Búsqueda de ubicaciones comunes de almacenamiento de contraseñas (T1555):** Los atacantes buscan archivos y otros lugares donde los usuarios puedan haber guardado sus contraseñas en texto plano.

Una vez que el malware está instalado, el atacante necesita una forma de comunicarse con él para enviar comandos y recibir datos. Para ello, establecen un canal de comunicación de comando y control, a menudo utilizando:

- **Protocolos de capa de aplicación (T1071):** Se utilizan protocolos comunes como HTTP o DNS para ocultar el tráfico malicioso y evitar la detección por parte de los sistemas de seguridad.
- **Protocolos no estándar (T1095):** Se emplean protocolos personalizados para la comunicación entre el host y el servidor del atacante, lo que dificulta aún más la detección.
- **Tunelización de protocolos (T1572):** Se encapsula el tráfico de C2 dentro de otro protocolo para evadir los controles de red y mantener una comunicación encubierta.

7. Colección e Impacto:

En la fase final del ataque, el ciberdelincuente logra su objetivo, que puede ser:

- **Cifrar datos (T1486):** En los ataques de ransomware, los datos de la víctima se cifran para exigir un rescate.
- **Eliminar o cifrar backups (T1490):** Se destruyen las copias de seguridad para evitar que la víctima pueda recuperar sus datos sin pagar el rescate.
- **Destruir datos y archivos (T1485):** En algunos casos, el objetivo es simplemente causar el mayor daño posible, destruyendo datos y sistemas críticos.
- **Exfiltrar datos (T1041):** Se roban datos confidenciales, como información de clientes o propiedad intelectual, para venderlos en la dark web o utilizarlos para otros fines maliciosos.

La Higiene de Ciberseguridad: La Mejor Defensa

La buena noticia es que, según los expertos, el 98% de los ciberataques se podrían evitar con una adecuada higiene de ciberseguridad. Esto implica implementar una serie de controles y buenas prácticas, como:

- **Autenticación multifactor (MFA):** Requerir una segunda forma de verificación además de la contraseña dificulta enormemente que los atacantes accedan a las cuentas, incluso si han robado las credenciales.
- **Principios de confianza cero (ZTNA):** No confiar en nadie por defecto, ni siquiera en los usuarios dentro de la red, y verificar siempre la identidad y los permisos antes de conceder el acceso a los recursos.
- **Soluciones anti-malware de nueva generación:** Utilizar herramientas avanzadas que puedan detectar y bloquear no solo el malware conocido, sino también las amenazas nuevas y desconocidas.
- **Mantener la infraestructura actualizada:** Aplicar los parches de seguridad de forma regular para corregir las vulnerabilidades antes de que puedan ser explotadas por los atacantes.

No obstante, la implementación de estas buenas prácticas debe venir acompañada de una cobertura adecuada de su aplicación, misma que cubra al 100% de los usuarios, el 100% de la infraestructura y al 100% de las aplicaciones.

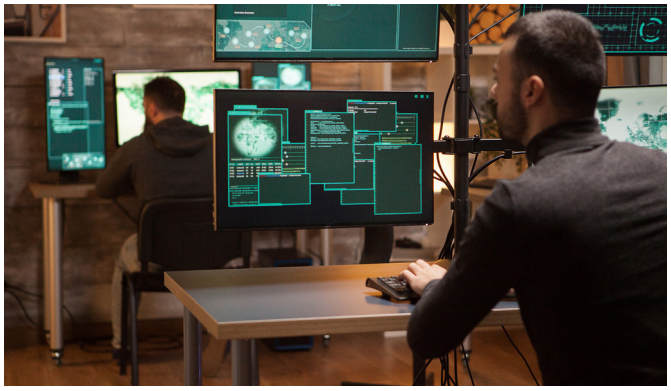
En definitiva, la ciberseguridad es un desafío constante que requiere un enfoque proactivo y multifacético. Comprender la anatomía de un ciberataque es el primer paso para construir una defensa sólida y proteger los activos más valiosos de una organización en el complejo panorama digital actual.

Seguridad física + Seguridad Lógica: Un binomio inseparable en la era de la transformación

Norman Romero
Vicepresidente de Prevención de Fraudes y Seguridad de Banco Internacional

La convergencia de seguridad (integral), junto a los sistemas de tecnología de la información (IT), con sistemas de tecnología operacional (OT), utilizados para supervisar eventos, procesos, dispositivos y realizar ajustes en las operaciones de las organizaciones, instituciones, empresas e industrias es ya una realidad que la estamos atravesando y cada vez con mayor velocidad, ya que así lo demanda el día a día. En este sentido, este artículo busca transmitir mi visión sobre la seguridad en tiempos de transformación digital.

Este proceso es la consecuencia lógica de la incorporación cada vez más intensa de tecnología a los negocios de todo tipo con el objetivo de mejorar radicalmente su rendimiento y, en los casos más extremos, cambiar los procesos estratégicos del negocio e incluso, la propuesta de negocio. Esta continua y progresiva conectividad, ha puesto sobre el tapete un nuevo modelo de seguridad, que va más allá de la seguridad física (protección de activos tangibles), y que pone también el foco en evitar la pérdida de datos (protección de activos intangibles), garantizando que la información fluya, que esté disponible, que las organizaciones, instituciones, y los negocios puedan beneficiarse de su análisis, y en evitar las vulnerabilidades derivadas de la conexión a la red.



Hoy es imposible desligar la seguridad física de la seguridad lógica. Por ello, se debe seguir construyendo y fortaleciendo una propuesta de seguridad evolutiva, que integre desde lo holístico la seguridad y ahora la ciberseguridad.

La integración como valor

Esta propuesta de valor permite un enfoque global que implica a las áreas de Seguridad Física y Lógica planificar un mapa de ruta que permita al Estado, sociedad y empresas ser cada vez más seguras y eficientes.

> **Es indispensable fortalecer las capacidades de las entidades financieras para llevar a cabo proyectos de ciclo completo, desde el análisis de los riesgos y vulnerabilidades físicas y lógicas, hasta el apoyo para el diseño, despliegue, gestión y monitorización de toda su operación de seguridad (Ciclo de Deming).**

De esta forma contar con una capacidad óptima para identificar, prevenir, y de ser el caso responder de forma integral a riesgos y amenazas. Por lo tanto, la simbiosis e integración es una virtud que requieren las instituciones para lograr cambios en beneficio de estas, lo cual servirá, entre otras cosas, para modelar la forma de gestionar los riesgos que normalmente son cambiantes, intimidantes y desafiantes.

Hemos tenido éxitos en nuestras gestiones, pero también fracasos, y de estos, aprendizajes. Una visión amplia de integración e interdependencia nos nutre a todos y debemos unir esfuerzos para fortalecernos desde el Estado con espacios como Comités de Seguridad sectoriales ,tanto en lo público como en lo privado, que generen directrices como sociedad y concientizar a nuestros usuarios, que normalmente son el eslabón más débil de la cadena. De aquí la importancia de la capacitación a los usuarios de forma continua por diversas aristas y usos.

Desde el punto de vista de la seguridad física, los tradicionales sistemas de seguridad están incorporando progresivamente una mayor capacidad de captura de datos, a la que se suma una cada vez más alta capacidad de comunicación entre todos los sistemas.

Estamos hablando de sistemas de control de accesos de personas o vehículos mediante biometría, tarjetas sin contacto, tags, chips, passwords o tokens; sistemas de protección perimetral CCTV con analíticas de vídeo, cables sensores, vallas y suelos sensorizados, microondas, infrarrojos, radar; sistemas de videovigilancia CCTV, en interiores o exteriores, con analíticas, PTZ, domos, minidomos, cámaras 360º/180, progresivamente seguimientos automáticos, rondas; sistemas anti intrusión, diversidad de sensores: IR, radar, algoritmos basados en AI, combinaciones con CCTV, reducción de falsos positivos en alarmas; sistemas de detección de incendios, integración de centrales de alarma homologadas, sensores analógicos y digitales, detectores de gases y humo, etc.

Esta mayor conectividad, unida a la necesidad de obtener el máximo rendimiento de los datos que proporcionan los sistemas, hace imprescindible abordar, de forma coordinada e integrada la seguridad física y la seguridad lógica o ciberseguridad.

Hasta hace un tiempo los ciberataques sólo afectaban al entorno IT (ERP, CRM, plataforma email, paquetes ofimáticos, etc.) pero el entorno IOT (Internet de las cosas), al estar actualmente más conectado e integrado, también se ha vuelto más vulnerable.

Es decir, tanto en IT como en IOT deben activarse las combinaciones adecuadas, de las más avanzadas estrategias de protección, como los detectores de intrusión lógica (IDS/IPS), y técnicas, como microsegmentación de redes, Network Access Control (NAC), Advanced Malware Protection (AMP), Security Information and Event Management (SIEM), soluciones como TrustSec (ISE) de CISCO o similares, además de la implantación interna o externa de un Security Operations Center (SOC) para la monitorización y gestión de eventos, la planificación, elaboración y aplicación de planes de contingencia etc.

Las empresas, y especialmente el sector financiero, avanzan con paso firme hacia la digitalización a través de la incorporación cada vez más intensa de tecnologías de la información.

Se abren múltiples posibilidades a los negocios con la obtención de información de valor para mejorar su eficiencia y los servicios y productos que ofrecen a sus clientes. La seguridad, en su doble perspectiva física y lógica, se vislumbra como un facilitador para que todo ese proceso fluya.

En síntesis, se hace cada vez más importante y prioritario que la Seguridad Física junto con la Seguridad Lógica o Ciberseguridad, miren desde un enfoque holístico a las organizaciones, para que mediante un esquema en profundidad, ir colocando las capas necesarias para proteger los activos tangibles e intangibles de nuestras organizaciones.

La Necesidad de una Estrategia de Seguridad Nacional

Marcelo Romero Almeida
Exdirector del Centro de Estudios y Pensamiento Estratégico (CESPE) de la Universidad de las Fuerzas Armadas (ESPE)

La Seguridad Nacional como un derecho ciudadano

La Seguridad Nacional es un derecho fundamental del ser humano y se orienta para alcanzar los altos fines de la sociedad (intereses nacionales). La seguridad es una necesidad, una aspiración y un derecho inalienable para todas las personas, con una connotación de garantía, protección o tranquilidad frente a obstáculos y amenazas contra las personas, las instituciones y los bienes esenciales de una sociedad. Todo Estado y sus gobiernos, tienen el deber de proteger a su población de amenazas de orden interno y externo.

Así lo consagra la Constitución de la República del Ecuador en su artículo 3, cuando establece como deber primordial del Estado "Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción."

Este deber de los Estados no puede desconocer la necesidad de establecer estrategias conjuntas y regionales. Así lo reconoció la Asamblea General de la Organización de Naciones Unidas cuando a inicios del siglo aceptó que todas las amenazas son transnacionales y establecieron que era necesario "un amplio debate" sobre cómo defender, no solamente la supervivencia de la especie, sino su convivencia en paz. Era necesario llegar a consensos en materia de seguridad, como lo estableció la resolución 60/1 de la Asamblea General de la ONU "el desarrollo, la paz, la seguridad y los derechos humanos se refuerzan mutuamente, la mejor manera en que se puede proteger un Estado no es nunca actuando completamente aislado (…)."[1]

Además de la guerra y los conflictos internacionales, se aceptó que se debían considerar las armas de destrucción en masa, la delincuencia organizada, los disturbios civiles, la pobreza, las enfermedades infecciosas mortales y la degradación del medio ambiente, ya que también estas pueden tener consecuencias catastróficas. Todas estas amenazas pueden socavar a los Estados como unidades básicas del sistema internacional.

Las amenazas a la seguridad regional [2]

Más de medio siglo después de la declaración de la guerra contra las drogas, América Latina lucha por controlar el estallido de violencia que viene de la mano con el narcotráfico. Aunque el crimen organizado relacionado con las drogas ha tenido picos de violencia notorios en el pasado, sobre todo en Colombia y México, nunca se había extendido tanto y rara vez había penetrado tan profundamente.

Los grupos criminales se han dividido, multiplicado y diversificado, adaptándose a las condiciones del mercado, y se han involucrado en nuevos negocios ilegales, incluyendo la extorsión, la minería ilegal, la trata de personas. Donde encuentran comunidades pobres y desprotegidas, los grupos criminales actúan como empleadores; donde hay presencia de funcionarios estatales, los coaccionan y corrompen.

El mapa del narcotráfico en América Latina se ha transformado en las décadas transcurridas desde que surgieron las primeras rutas de suministro desde los Andes hacia EE. UU., aunque Colombia y México siguen siendo el corazón del negocio de las drogas, una de las principales rutas para llegar a EE. UU. y en particular a Europa, se extiende por el Pacífico, abarcando países que en gran medida no habían sido afectados por el tráfico ilícito, como Costa Rica y Ecuador. En cada uno de ellos se han registrado fuertes aumentos de las tasas de violencia; Ecuador fue en 2024 la nación más violenta de Sudamérica, y en lo que va del año 2025 se romperá cualquier registro previo de violencia.

Comprender cómo se produjo esta oleada de delincuencia es fundamental para detenerla. El narcotráfico se ha adaptado a

[1] Naciones Unidas, Documento Final de la Cumbre Mundial 2005, Resolución A/RES/60/1, aprobada por la Asamblea General el 16 de septiembre de 2005, párr. 48.

[2] International Crisis Group, Curbing Violence in Latin America's Drug Trafficking Hotspots, Informe N.º 108 (11 marzo 2025), p. 29.

las amenazas de las operaciones de seguridad, volviéndose más flexible y resistente. En lugar de organizaciones jerárquicas que podían desmantelarse una vez identificados sus líderes, el narcotráfico funciona cada vez más a través de redes de proveedores que subcontratan cada etapa de la ruta a otros operadores más pequeños. A nivel local, los grupos nacionales manejan la producción o garantizan el paso seguro de la droga por un corredor determinado de tráfico; las bandas urbanas son contratadas por aliados criminales más grandes para que presten servicios logísticos de pequeña escala, como el contrabando de drogas a través de puertos. Estas bandas reciben su pago en droga por lo que se desencadena la violencia al momento de disputar los mercados para el microtráfico, que les permita monetizar sus ganancias.

Al tratarse de un problema regional o global que involucra a diversos actores, la solución debe pasar por una cooperación internacional en la que todos los actores, países productores, de tránsito, consumidores, paraísos fiscales se comprometan a tener una sola política, caso contrario todos los esfuerzos serán estériles.

La crisis de seguridad en el Ecuador[3]

Ecuador es uno de los centros de tráfico de drogas más importantes de la región, utilizado para enviar cocaína colombiana y peruana a Europa, México y Centroamérica. En los últimos años, a los carteles internacionales y a sus representantes locales se les han unido una nueva generación de grupos criminales conocidos en Ecuador como "mafias", que se apoderaron del sistema penitenciario al tiempo que creaban redes de bandas en las calles. Todas estas redes criminales se han beneficiado de una corrupción rampante que ha contaminado la seguridad, la justicia, las instituciones gubernamentales y la política del país.

Ecuador, limita con los dos mayores productores de cocaína del mundo: Colombia al norte y Perú al este y al sur. Esto, combinado con su extensa costa occidental a lo largo del océano Pacífico, lo ha convertido en uno de los principales puntos de envío para el comercio mundial de cocaína. En particular, la ciudad de Guayaquil se ha convertido en un punto crucial de transbordo de la droga hacia Europa, mientras que las provincias costeras de Manabí y Esmeraldas son importantes corredores de tráfico utilizados para llegar a México y Centroamérica.

En Colombia, la política de "Paz total" implementada por el gobierno del presidente Petro, ha sido incapaz de lograr los objetivos establecidos por su gobierno y ha estimulado el cultivo de vastas extensiones de hoja de coca, ya que no se criminaliza la producción de la hoja de coca, sino las actividades ilícitas de narcotráfico. Como consecuencia de ello a finales del año 2023 los cultivos de coca se incrementaron a más de 253.000ha y en el último informe de la UNODC se informa que los cultivos superan las 260.000 HA con una producción superior a las 2800 TM anuales de cocaína.

Las acciones implementadas por los gobiernos de Colombia tienen su repercusión directa sobre nuestro país y su incidencia se puede observar en la siguiente Tabla, que describe la línea temporal del crimen organizado en Ecuador.

El crimen organizado en el Ecuador

Periodo	Eventos Clave	Impacto
1970-1990	Los carteles de Medellín y Cali utilizan Ecuador como punto de tránsito y centro de contrabando de precursores químicos.	Expansión del narcotráfico y consolidación de rutas ilícitas.
1990-2000	Ingreso de las Fuerzas Armadas Revolucionarias de Colombia (FARC) en territorio ecuatoriano, estableciendo bases en la frontera y rutas de narcotráfico. Ingreso de paramilitares colombianos.	Militarización de la frontera y fortalecimiento del crimen organizado vinculado a actores armados.
2000-2010	Crecimiento de bandas callejeras y violencia urbana. Legalización de pandillas como Latin Kings dentro de un proceso de pacificación. Aparición de redes criminales internacionales de Colombia y México.	Reducción temporal de homicidios. Mayor infiltración del narcotráfico internacional.
2010-2020	Salida de redes extranjeras y crecimiento de grupos narcotraficantes nacionales. Consolidación del control de prisiones por mafias carcelarias.	Surgimiento de estructuras criminales autóctonas y fortalecimiento del crimen dentro del sistema penitenciario.
2021-2023	Fragmentación de Los Choneros, enfrentamientos entre disidencias y escalada de violencia en cárceles y calles. Asesinato de un candidato presidencial en 2023.	Crisis de seguridad sin precedentes y aumento de la violencia política.
2024 - actualidad	Implementación de operativos militares en cárceles y calles para recuperar el control del país.	Mayor militarización de la seguridad interna y redefinición de estrategias de lucha contra el crimen organizado.

[3] InSight Crime, «Ecuador – Noticias sobre crimen organizado en Ecuador», disponible en https://www.insightcrime.org/es/noticias-crimen-organizado-ecuador/ecuador

Grupos criminales que operan en el país

Los dos grupos más grandes y sofisticados que operan actualmente en el país son Los Choneros y Los Lobos. Estos grupos trabajan tanto con narcotraficantes ecuatorianos como internacionales. Entre ellos se encuentran el Cartel de Sinaloa y el Cartel de Jalisco Nueva Generación de México, y la mafia albanesa; aunque existen otros grupos internacionales con presencia significativa en Ecuador, como facciones disidentes de las FARC, Frente Oliver Sinisterra y los Comandos de la Frontera, que permanecen activos a lo largo de la frontera colombiana. Además, el Ejército de Liberación Nacional (ELN), otro grupo rebelde colombiano, ha utilizado Ecuador como refugio.

Las fuerzas de seguridad

La Policía Nacional es la principal institución dedicada a luchar contra el crimen organizado en el país, sin embargo, a medida que el crimen organizado transnacional se ha expandió en el país, los escándalos de corrupción en la institución se incrementaron. Por ello, y dada la relación tensa entre el gobierno de Rafael Correa y la Policía, a partir del 2012 se involucró a las Fuerzas Armadas en tareas relacionadas con la seguridad pública y en las operaciones antinarcóticos.

El involucramiento cada vez mayor en estas actividades ha permitido que los grupos criminales exploten con éxito a funcionarios militares, lo que ha permitido que las bandas y los traficantes puedan obtener armas y municiones pertenecientes a las Fuerzas Armadas y que el personal militar se haya involucrado en actividades ilícitas relacionadas. A partir de enero del 2024, el despliegue de militares en los centros de privación de libertad para acabar con el dominio de las bandas y aliviar la notoria corrupción de las autoridades penitenciarias, provocó denuncias de abusos generalizados de los derechos humanos y preocupación por la creciente corrupción entre sus miembros. Actualmente, aproximadamente entre el 12 y el 15% de los efectivos de las FFAA se encuentran involucrados directamente en el control carcelario, reduciendo significativamente sus capacidades para el cumplimento de sus tareas específicas como son el control del cordón fronterizo.

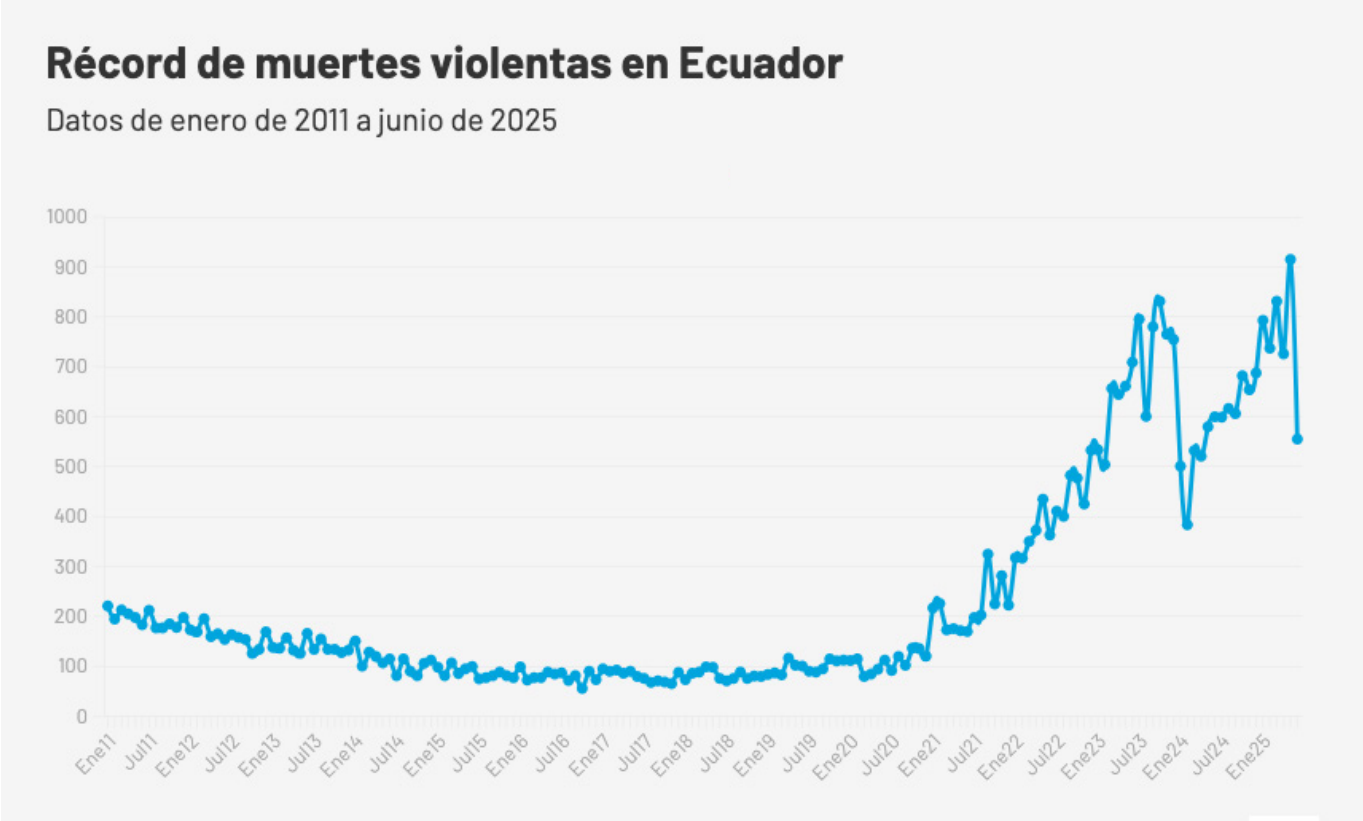
Sistema judicial

El sistema judicial ecuatoriano enfrenta altos niveles de corrupción y frecuentemente es influenciado por el crimen organizado y élites corruptas. Entre 2023 y 2024, investigaciones como los casos Metástasis, Purga, Encuentro y Ligados evidenciaron esta situación. A ello hay que agregarle la incertidumbre institucional que vive la Fiscalía General del Estado, que se encuentra sin su titular desde marzo de 2025, y cuya nueva máxima autoridad podría ser designada en marzo de 2026.
Sistema Penitenciario

El sistema penitenciario del Ecuador se ha convertido en uno de los más violentos del mundo a causa del hacinamiento crónico, falta de recursos y corrupción, lo que ha favorecido la aparición de mafias carcelarias. Las disputas entre estas mafias entre 2019 y 2023 provocaron cientos de muertes y derivaron en que, en enero de 2024, las fuerzas armadas intervengan en el sistema penitenciario.

Situación interna de Ecuador al 2025

Como consecuencia de la grave crisis de seguridad, en el mes de enero del 2024 el presidente Noboa declaró la existencia de un Conflicto Armado No Internacional, lo que permitió la movilización de las Fuerzas Armadas y la militarización del sistema carcelario.
En 2025, Ecuador atravesó el inicio de año más violento desde que hay registros públicos. Entre enero y febrero, se cometieron 1.529 asesinatos. En promedio, cada día en Ecuador mueren violentamente 26 personas. Febrero de 2025, con 736 muertes violentas, es el sexto mes más violento desde enero de 2011. En promedio, en enero de 2025 se cometieron 24 asesinatos cada día y en febrero de 2025, 26.



Elaborado por: Primicias
Fuente: Ministerio del Interior

La grave situación descrita nos lleva a la formulación del siguiente cuestionamiento, el cual merece una adecuada respuesta por parte de los responsables por la administración del Estado:

¿El Ecuador dispone de una estrategia nacional que oriente a sus componentes a la consecución de los grandes intereses nacionales y a la solución de los graves problemas que aquejan a la sociedad?

Para dar una respuesta a estos cuestionamientos, es necesario recalcar que la conducción política de un Estado no puede ser concebida sin que de por medio los responsables, no hayan formulado una estrategia nacional que oriente claramente los derroteros que la sociedad y el gobierno, deban seguir para alcanzar los objetivos que se han propuesto.

Para la formulación de una estrategia nacional, se deben considerar los siguientes aspectos:

La estrategia formulada en el más alto nivel – político – de la toma de decisiones del Estado, puede ser definida como el empleo de todos los instrumentos que dispone un Estado para apoyar a la visión estratégica en el concierto internacional, que le permita alcanzar de la mejor manera los objetivos nacionales que se ha impuesto.

Es importante recordar, que para la formulación de una estrategia, incluida la estrategia nacional, requiere de un cálculo del balance continuo que debe existir entre las distintas variables que la componen: las formas (método para el empleo de los recursos disponibles para alcanzar los objetivos previstos); los medios disponibles (recursos humanos, financieros, materiales, etc); los fines (objetivos a ser alcanzados); y, los riesgos relacionados con la formulación y aplicación de esta estrategia. Todo ello dentro de una evaluación permanente del entorno estratégico a nivel interno y externo.

La formulación de una estrategia arranca con la comprensión del propósito del país, lo cual conlleva a la identificación de los intereses nacionales. Estos se entienden como la noción de las aspiraciones esenciales del país, mismas que deben ser identificadas, recogidas, perseguidas y protegidas por el Estado; por lo tanto, reflejan las ideas y aspiraciones sociales, políticas, económicas y ambientales del individuo y la sociedad civil en su conjunto, los cuales guían y fundamentan el soporte político y legítimo al Estado y sus instituciones para su persecución permanente a nivel nacional e internacional.

Los objetivos nacionales, son aquellos que se derivan directamente de los intereses nacionales, y otorgan sustancia a las aspiraciones e ideas sintetizadas en los intereses nacionales. Los objetivos nacionales poseen el carácter de "permanentes" bajo la categorización conceptual constitucional de los deberes primordiales del Estado frente a la sociedad civil.

Los objetivos actuales, se constituyen en la acción práctica del gobierno de turno para contribuir a la búsqueda de los intereses nacionales en el horizonte temporal del periodo gubernamental basados en la situación de coyuntura presente. Los objetivos actuales deben ser plasmados en el Plan Nacional de Desarrollo de cada gobierno, el cual a su vez guía la planificación de los diferentes sectores y el desarrollo de la política en torno a la problemática social.

Las funciones del Estado deben formular y evaluar permanentemente estrategias sectoriales específicas para alcanzar los objetivos establecidos por la política nacional en el ámbito de su responsabilidad y abordar aquellas cuestiones de importancia nacional. Este proceso requiere del compromiso y el esfuerzo continuo de los responsables, ya que el ambiente de la seguridad, con sus componentes nacionales e internacionales, está en constante evolución, por lo que es necesario una evaluación permanente del riesgo, como parte del proceso de formulación de la estrategia.

Durante el proceso de formulación de la estrategia nacional, los gobernantes y estrategas deben conducir una evaluación de la estrategia diseñada, que permita determinar su idoneidad; aceptabilidad; y, factibilidad.

Este análisis se utiliza además para identificar y evaluar los posibles efectos colaterales de segundo y tercer orden involucrados en la implementación de la estrategia, por ejemplo, el impacto de la estrategia sobre los diferentes grupos sociales, las distintas regiones, sobre la economía; o el impacto potencial sobre los recursos, o restricciones derivadas de la implementación de la estrategia.

Idealmente, este riguroso proceso analítico nos conducirá al desarrollo de la Estrategia de Seguridad Nacional y estrategias sectoriales derivadas tales como la Estrategia de Defensa Nacional, la estrategia de Inteligencia Nacional, la estrategia nacional de Cyberseguridad, entre otras.

Conclusiones

La Seguridad es un derecho fundamental del ser humano y la seguridad nacional se orienta para alcanzar los intereses nacionales. Todo Estado y sus gobiernos, tienen el deber de proteger a su población de amenazas de orden interno y externo. Por ello, el Estado es el principal responsable de la seguridad de su población y territorio.

La región latinoamericana, a pesar de los múltiples esfuerzos desarrollados, aún lucha por controlar el estallido de violencia que viene de la mano con el narcotráfico. Los grupos criminales se han adaptado a las condiciones del mercado, diversificando su tradicional oferta del tráfico de sustancias ilegales hacia nuevos negocios ilegales, incluyendo la extorsión, la minería ilegal, la trata de personas.

La solución de este problema no pasa solamente por el empleo de la fuerza militar y/o policial. Es muy importante comprender cómo se produjo esta oleada de delincuencia para poder detenerla. Por las experiencias vividas, es necesario un fortalecimiento de los sistemas de inteligencia para generar una mejor acción de la fuerza pública; el apoyo estatal para la atención de las necesidades básicas de las poblaciones marginales; el control del tráfico de armas, municiones y explosivos; y, en determinadas condiciones, el desarrollo de negociaciones, contribuirán a la reducción de la violencia.

Ante la delicada situación política que vive el país, derivada de la crisis social, económica y de seguridad, el Estado debe propender a desarrollar las acciones que permitan la normalización de la situación. Surge la necesidad de trabajar fuertemente desde el ámbito de la conducción política del estado, para formular una estrategia nacional orientada a la consecución de los objetivos nacionales.

Finalmente, es necesario también iniciar un proceso fortalecimiento de la cultura de seguridad, que permita que los responsables de la conducción política puedan realizar el diagnóstico de la configuración estructural de las instituciones del Estado, que permita fortalecer desde adentro las capacidades institucionales incluidas su cultura organizacional.

De la inmediatez al control: Seguridad y confianza en los pagos con PIX

Luana Romero de Souza
Consultora Internacional en Integridad, Compliance y Seguridad en Sistemas Financieros Digitales

Inmediatez y confianza en los pagos digitales

La velocidad en las transacciones financieras se ha convertido en un imperativo global. Los sistemas tradicionales, con procesos lentos y costos elevados, ya no satisfacen las necesidades de la sociedad moderna. En este contexto, Brasil desarrolló el PIX, un sistema de pagos instantáneos que no solo agiliza las transacciones, sino que integra regulación, seguridad y control, convirtiéndose en un ejemplo de innovación pública.

El PIX ha transformado la relación de los ciudadanos con el dinero, ofreciendo acceso inmediato, inclusión financiera y confianza. Sin embargo, su valor va más allá de la velocidad: el verdadero diferencial está en cómo este sistema se diseñó para prevenir delitos financieros, fortalecer la integridad del sistema y garantizar la transparencia.

Orígenes de PIX: innovación pública con propósito

La necesidad de modernizar el sistema financiero brasileño llevó al Banco Central do Brasil (BCB) a desarrollar el PIX. Antes de su creación, millones de personas enfrentaban exclusión financiera, altos costos en transacciones y falta de interoperabilidad.

El Banco Central adoptó un enfoque innovador, al construir una infraestructura pública neutral, con el objetivo de garantizar que todos los participantes, desde grandes bancos hasta fintechs, operen bajo los mismos estándares de seguridad y transparencia.

Este modelo no solo promovió inclusión, sino que incorporó mecanismos de control y supervisión robustos, diseñados para minimizar riesgos y prevenir delitos financieros desde la base del sistema.

El PIX y la prevención de delitos financieros

La velocidad en los pagos introduce riesgos inherentes: fraudes, suplantación de identidad, transferencias erróneas y potencial uso para lavado de dinero y financiamiento del terrorismo. El PIX se distingue porque la prevención de delitos financieros está integrada desde su concepción, reforzando la confianza de los usuarios y la integridad del sistema.

Algunas de las estrategias implementadas incluyen:

- **Supervisión centralizada y colaboración institucional:** El Banco Central coordina con la Unidad de Inteligencia Financiera (COAF), la Policía Federal y otras entidades, creando un ecosistema donde la detección y la respuesta a incidentes son inmediatas.
- **Regulación basada en riesgo:** Las instituciones financieras deben implementar políticas robustas de conozca a su cliente (KYC), monitoreo transaccional y reportes de operaciones sospechosas, con enfoque en riesgo proporcional al tipo de operación y perfil del cliente.
- **Educación y concienciación del usuario:** Campañas masivas enseñan cómo operar con seguridad, identificar intentos de fraude y confirmar siempre la autenticidad del receptor de pagos. La educación financiera es un pilar clave de la confianza en el PIX.
- **Mecanismos de reversión y protección:** Las operaciones fraudulentas pueden revertirse mediante procedimientos establecidos, garantizando que los usuarios tengan recursos efectivos para proteger sus fondos.

Este enfoque demuestra que la innovación tecnológica no puede separarse de la regulación y el control, y que la velocidad de las transacciones no debe comprometer la seguridad ni la integridad del sistema.

Fraudes y riesgos: cómo el PIX enfrenta los desafíos

A pesar de sus medidas preventivas, el PIX ha sido objeto de intentos de fraude, que se concentran principalmente en:

- **Ingeniería social y suplantación de identidad:** delincuentes persuaden a usuarios para que envíen fondos a cuentas fraudulentas.
- **Phishing y aplicaciones maliciosas:** creación de plataformas falsas que simulan ser bancos o servicios de pago.
- **Errores de claves y datos de receptor:** transferencias realizadas a destinatarios incorrectos.
- **Movimientos ilícitos de dinero:** intentos de usar el sistema para lavado de activos.

Frente a estos desafíos, la combinación de regulación estricta, monitoreo en tiempo real y la educación financiera han permitido que el sistema mantenga una tasa de fraude controlada en comparación con su rápida adopción. La respuesta institucional rápida y coordinada es clave para sostener la confianza del público.

Confianza, regulación y gobernanza

El éxito del PIX se basa en la construcción de confianza social, donde el Banco Central actúa como garante de estabilidad y transparencia. La regulación no se limita a establecer normas: define responsabilidades claras, mecanismos de control y protocolos de supervisión que fortalecen la resiliencia del sistema.

El enfoque brasileño combina:

1. **Neutralidad institucional:** la infraestructura es de carácter público, evitando conflictos de interés que puedan comprometer la transparencia.
2. **Control regulatorio constante:** auditorías, monitoreo y reportes obligatorios aseguran que todas las operaciones cumplan con estándares de integridad.
3. **Educación del usuario:** fortalecer el conocimiento financiero de los ciudadanos es parte de la política de prevención de delitos.

Este modelo demuestra que inmediatez y confianza son inseparables, y que la seguridad no es un complemento, sino un elemento central de la innovación en pagos.

Impacto económico y social del PIX

Más allá de la seguridad, el PIX ha generado un impacto profundo en la economía brasileña:

- **Inclusión financiera masiva:** millones de ciudadanos acceden por primera vez a pagos digitales.
- **Formalización de la economía:** pequeñas empresas y trabajadores informales pueden operar dentro del sistema financiero.
- **Reducción de costos y eficiencia:** pagos instantáneos reducen la dependencia de efectivo y los costos de transacción.
- **Innovación tecnológica y competencia:** fintechs y bancos digitales desarrollan nuevos servicios sobre la infraestructura PIX, estimulando un ecosistema más dinámico y competitivo.

El sistema demuestra que la innovación puede ser inclusiva y segura, y que la regulación no inhibe la competitividad, sino que la fortalece.

Proyección internacional: modelo para la región

El PIX ha trascendido fronteras como ejemplo de innovación regulada. Organismos como el Banco de Pagos Internacionales (BIS) y el Fondo Monetario Internacional (FMI) reconocen el modelo brasileño por su capacidad de combinar velocidad, inclusión y control.

Países como Colombia, Chile, Ecuador, México, Paraguay y Perú estudian la experiencia brasileña para desarrollar sistemas propios de pagos instantáneos que incorporen mecanismos de prevención de fraudes y delitos financieros.

El potencial del PIX internacional — pagos transfronterizos instantáneos — apunta a fortalecer la integridad y eficiencia regional, reduciendo costos de remesas y promoviendo transparencia en flujos financieros internacionales.

El futuro del PIX: regulación, prevención y sostenibilidad

El Banco Central continúa expandiendo el ecosistema con un enfoque claro: innovación, seguridad y prevención de delitos. Las próximas etapas incluyen:

- **Automatización de procesos de control y monitoreo,** apoyada en inteligencia artificial y análisis de riesgos.
- **Expansión internacional,** integrando estándares de seguridad y prevención de lavado de dinero a nivel transfronterizo.
- **Fortalecimiento de la educación financiera,** para asegurar que la adopción masiva no comprometa la seguridad individual ni sistémica.

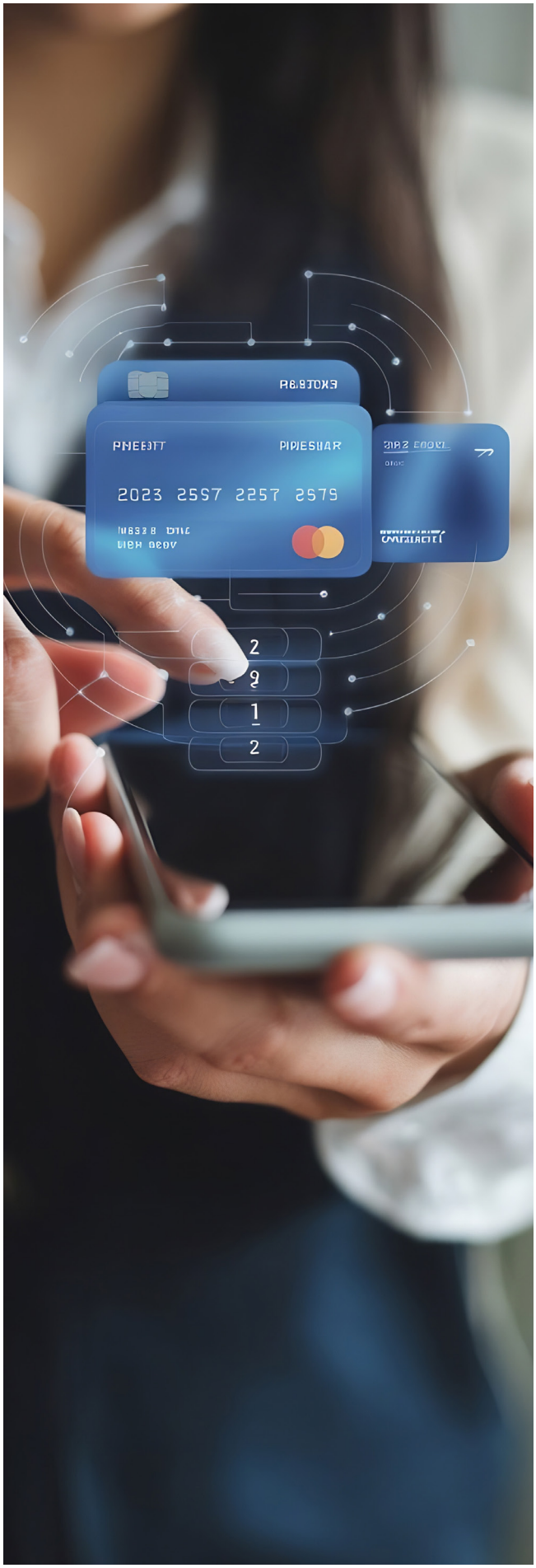
El legado del PIX se construye sobre un equilibrio entre inmediatez, control y confianza, demostrando que la innovación regulada puede ser un motor de transformación social y económica.

Conclusiones: la confianza como moneda del futuro

El PIX es mucho más que un sistema de pagos: es un instrumento de gobernanza y confianza pública. Su éxito radica en la armonía entre velocidad, inclusión y control, y en su capacidad de prevenir fraudes y delitos financieros desde el diseño.

Brasil demuestra que la innovación tecnológica no está reñida con la regulación, sino que requiere de ella para sostener la integridad del sistema y la confianza de los ciudadanos.

La verdadera innovación no reside únicamente en transferir dinero más rápido, sino en crear un ecosistema confiable y seguro, donde cada transacción protege a las personas y fortalece la economía. El PIX enseña que, en la era digital, la confianza es la moneda más valiosa.



Seguridad bancaria y pagos interoperables en el Ecuador: desafíos jurídicos frente al fraude electrónico y lecciones del modelo PIX de Brasil

Álvaro Lara Dillon
Abogado especializado en Derecho Financiero y Bancario. Máster en Derecho Financiero.

1. Arquitectura regulatoria del sistema de pagos interoperables en Ecuador

La interoperabilidad de los pagos en Ecuador se sustenta en un entramado normativo diseñado para armonizar eficiencia, inclusión financiera y seguridad. La piedra angular de esta arquitectura es la Resolución Administrativa No. BCE-GG-008-2025, mediante la cual el Banco Central del Ecuador (BCE), a partir de las disposiciones constantes en Resolución No. JPRM-2024-029-M de la Junta de Política y Regulación Monetaria (JPRM)[1], estableció el cronograma para la implementación del Sistema Integrador de Pagos (SIP) y su Red de Pagos Instantáneos (RPI). Esta resolución delimita también las condiciones de acceso, operación, compensación, liquidación y contingencia del sistema, previendo además aspectos de responsabilidad operativa y mecanismos de control técnico.

Paralelamente, la Junta de Política y Regulación Financiera (JPRF) ha expedido normativas que regulan la seguridad operativa, la protección de datos y los estándares de ciberseguridad aplicables a las entidades de servicios financieros tecnológicos. En este sentido, la Codificación de Resoluciones Financieras (Libro I) también exige la adopción de medidas técnicas, políticas de gestión de riesgos, auditoría y monitoreo continuo de operaciones electrónicas.

A esto se suma la Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos (Ley Fintech), publicada en 2022, que introdujo principios como la neutralidad tecnológica, la regulación basada en riesgos y la protección del consumidor financiero digital respecto a sus datos. Esta Ley, junto con su reglamento ejecutivo (Decreto 903 de 2023), delimita el rol de las entidades supervisoras, los requisitos de entrada para los proveedores tecnológicos, y establece la responsabilidad objetiva en ciertos casos de fallas tecnológicas y afectación a usuarios.

Finalmente, este conjunto normativo se encuentra en consonancia con la Política Pública para la Transformación Digital del Ecuador 2025–2030, que reconoce la interoperabilidad y la seguridad digital como ejes habilitantes para el desarrollo de servicios innovadores, y refuerza el deber del Estado de garantizar un entorno digital seguro, confiable y resiliente.

> **La existencia de múltiples órganos normativos –BCE, JPRFM, Superintendencias– configura un modelo de gobernanza regulatoria compartida, cuyo éxito dependerá de la coordinación técnica, la vigilancia sobre la ejecución y el cumplimiento de estándares internacionales sobre ciberseguridad y protección de datos.**

2. Fraude electrónico, responsabilidad jurídica y límites de cobertura en sistemas de pago interoperables

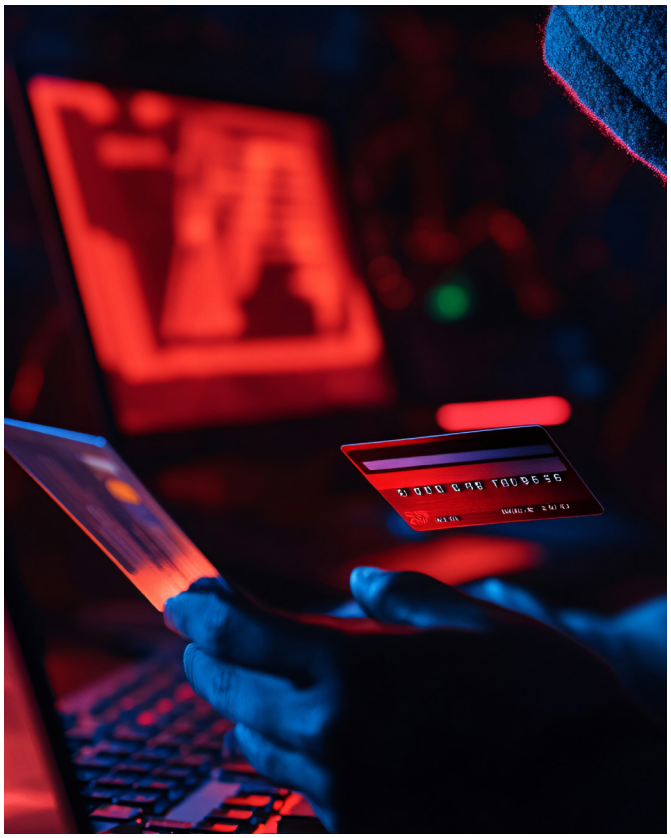
La modernización de los sistemas de pago ha traído consigo nuevos factores de riesgo jurídico, particularmente frente al fenómeno del fraude electrónico[2]. La masificación de servicios de pago instantáneo —basados en interoperabilidad— plantea desafíos en torno a la determinación de responsabilidad, la protección del usuario y los límites de cobertura ante ciberataques y suplantación de identidad.

[1] El marco jurídico no se agota en la normativa emitida por el BCE. La Junta de Política y Regulación Monetaria (JPRM), mediante la Codificación de Resoluciones Monetarias, ha emitido principios que respaldan jurídicamente la infraestructura del sistema de pagos, en particular los que garantizan la interoperabilidad de redes, la estandarización de procesos, la eficiencia del sistema y la inclusión financiera.

[2] En contextos bancarios y fintech, el fraude informático y la sustracción de información confidencial son los tipos penales más relevantes en el marco del Código Orgánico Integral Penal (arts. 190, 231 y 232), y se aplican a incidentes como transacciones electrónicas manipuladas, clonación de tarjetas, robo de credenciales, fraudes por phishing o ataques cibernéticos con propósitos de apropiación patrimonial.

En Ecuador, la Ley Fintech y su Reglamento establecen principios de protección al consumidor financiero digital, exigiendo a los prestadores de servicios tecnológicos que adopten medidas técnicas y organizativas adecuadas para prevenir incidentes de seguridad. Aunque esto implica un estándar de diligencia reforzada, no se consagra una obligación legal de cobertura o restitución automática en casos de fraude, salvo que se pruebe negligencia o incumplimiento normativo.

Por su parte, la Resolución No. BCE-GG-008-2025 faculta al Banco Central para implementar mecanismos de contingencia y control frente a la posibilidad de operaciones fraudulentas dentro del Sistema Integrador de Pagos (SIP). Sin embargo, esta normativa no desarrolla un régimen específico de responsabilidad objetiva o solidaria entre las entidades participantes frente al usuario afectado.



La Codificación de Resoluciones Financieras (JPRF) exige políticas de gestión de riesgos tecnológicos, mecanismos de monitoreo transaccional y sistemas de alertas para operaciones inusuales. Asimismo, impone a las entidades financieras la obligación de preservar la confidencialidad, integridad y disponibilidad de los datos y canales digitales. Sin embargo, la dispersión normativa y la falta de mecanismos expeditos de reversión y compensación —como sí lo contempla el modelo brasileño con su Mecanismo Especial de Devolución (MED)— debilita la posición del consumidor ante un evento fraudulento.

En la práctica, los usuarios que sufren fraudes deben iniciar reclamos administrativos ante sus instituciones financieras o acciones judiciales, lo cual dilata el acceso a una solución efectiva. El modelo ecuatoriano no contempla un fondo de compensación ni exige la contratación obligatoria de seguros para cubrir eventos de fraude en pagos interoperables.

El vacío jurídico sobre la responsabilidad compartida en arquitecturas distribuidas —donde intervienen múltiples actores: bancos, cooperativas, proveedores Fintech y el BCE como operador de la RPI— requiere una revisión normativa urgente, tanto para garantizar la seguridad jurídica del sistema como para proteger adecuadamente al usuario final.

3. Lecciones del esquema PIX en Brasil y su reciente ciberataque (junio 2025)

El sistema de pagos instantáneos PIX, lanzado por el Banco Central de Brasil (BCB) en noviembre de 2020, es hoy uno de los referentes más avanzados en interoperabilidad financiera de América Latina. Su arquitectura permite transferencias en tiempo real entre personas naturales, jurídicas e instituciones públicas, operando 24/7 a través de claves simples como el número de celular, el correo electrónico o el CPF. Ha sido considerado un instrumento eficaz de inclusión financiera, debido a su gratuidad para personas naturales y su facilidad de uso.

Desde su implementación, PIX ha estado respaldado por diferentes regulaciones en materia de ciberseguridad, responsabilidad institucional y mecanismos de resolución de disputas. El Mecanismo Especial de Devolución (MED), introducido en 2021, permite a los usuarios afectados por fraudes —como suplantación o ingeniería social— recuperar los fondos directamente del banco receptor, bajo ciertos supuestos y plazos.

En junio de 2025, el sistema sufrió su incidente más grave: un ciberataque masivo interno, que comprometió la integridad del sistema a través del acceso ilícito por parte de un operador acreditado (una Fintech regulada). Este ataque, documentado por medios como Infobae, Humanizing Banking y BeInCrypto, permitió desviar fondos que superaron los R$ 800 millones (aproximadamente unos US $100 millones). La causa raíz del ataque no fue un fallo técnico del sistema central del BCB, sino en una brecha de seguridad humana ocurrida dentro de uno de los nodos autorizados del sistema, específicamente una Fintech previamente validada para operar con PIX. Esta vulnerabilidad fue aprovechada para emitir órdenes de pago fraudulentas desde dentro del ecosistema, utilizando accesos legítimos pero comprometidos. A través de esa entidad participante, se generaron transacciones maliciosas en cascada, sin que el sistema central pudiera bloquearlas a tiempo, ya que desde el punto de vista operativo eran transacciones técnicamente válidas. Este evento demostró que, en arquitecturas distribuidas como la de PIX, el riesgo puede provenir no del núcleo del sistema, sino de sus bordes operativos, donde factores humanos, como una deficiente gestión de credenciales o la ausencia de controles internos eficaces, pueden tener efectos sistémicos.

La reacción del Banco Central de Brasil fue inmediata: suspensión de nodos, intervención administrativa, fortalecimiento de requisitos de ciberseguridad para participantes, y una reforma normativa que introdujo responsabilidad subsidiaria del BCB en casos de omisión o fallos estructurales de supervisión. Asimismo, se activaron protocolos de reversión vía MED y de cobertura por seguros previamente contratados por los actores participantes.

Este incidente evidenció que incluso un sistema robusto y maduro como PIX está expuesto a riesgos de tercerización, fraudes internos, y fallas en los controles de entrada (onboarding) de participantes. También demostró la importancia de contar con: (i) mecanismos normativos para la rápida reversión de fondos; (ii) mecanismos de reparación económica para eventos de fraude; (iii) exigencias reforzadas de responsabilidad jurídica en arquitecturas distribuidas.

Para el Ecuador, las lecciones del caso PIX son cruciales. Si bien el país ha adoptado una arquitectura técnica similar —basada en interoperabilidad abierta[3]—, carece de mecanismos compensatorios automáticos como el MED y no exige coberturas obligatorias para participantes en la Red de Pagos Instantáneos. Tampoco se ha regulado con precisión la responsabilidad solidaria en casos de fraude o ataque desde un nodo autorizado.

4. ¿Es el sistema ecuatoriano vulnerable a riesgos similares a los del caso PIX?

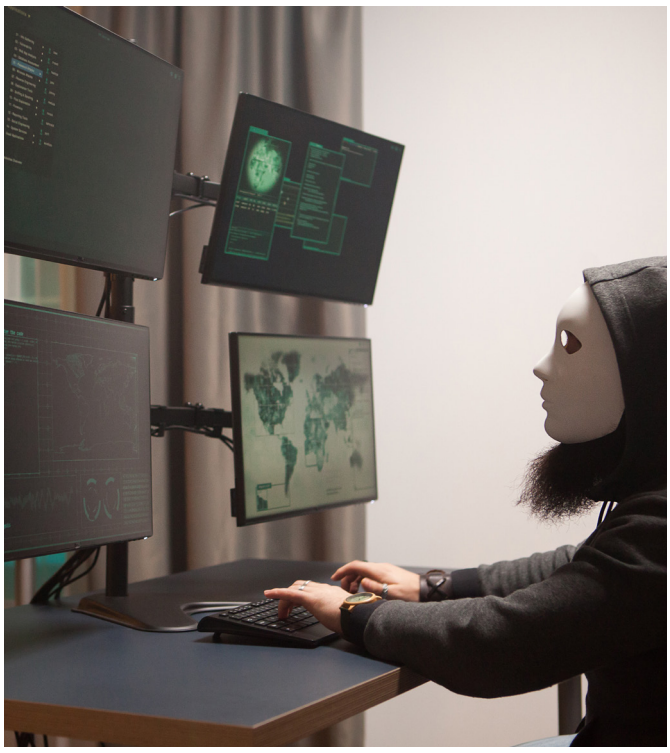
La experiencia brasileña con PIX permite evaluar, en clave comparativa, el grado de exposición del sistema ecuatoriano a riesgos estructurales, operativos y jurídicos en un entorno de pagos interoperables. Si bien existen diferencias institucionales y de madurez tecnológica, la arquitectura adoptada por Ecuador presenta similitudes relevantes que justifican una revisión crítica de su vulnerabilidad ante ataques cibernéticos y fraudes sistémicos.

Desde el punto de vista técnico, tanto PIX como la Red de Pagos Instantáneos (RPI) ecuatoriana operan bajo principios de interoperabilidad obligatoria, liquidación inmediata y alta disponibilidad, habilitados por interfaces abiertas (API) y esquemas distribuidos entre múltiples participantes. En ambos casos, el regulador central (BCB en Brasil y BCE en Ecuador) actúa como administrador de la plataforma de pagos, pero no controla directamente todos los puntos de acceso ni los sistemas de los actores integrados.
En lo normativo, Brasil ha complementado la regulación técnica con mecanismos robustos de reversión de fondos (MED) y estándares de ciberseguridad armonizados con la Lei Geral de Proteção de Dados (LGPD). Ecuador, en cambio, ha avanzado en la regulación habilitante, pero aún carece de normas que delimiten con claridad la responsabilidad por fallos o fraudes en arquitecturas distribuidas, especialmente en cuanto a:

- Responsabilidad solidaria entre los participantes del sistema.
- Reversión expedita de fondos en casos de fraude.
- Requisitos mínimos de cobertura y respuesta económica contra eventos de ciberataque.
- Protocolos de exclusión o suspensión inmediata de nodos comprometidos.
- Supervisión ex ante sobre criterios de admisibilidad técnica y reputacional.

El ataque a PIX en 2025 reveló que la vulnerabilidad no siempre proviene del sistema central, sino de los participantes conectados, incluyendo Fintech autorizadas o cooperativas con menor madurez digital. Esta situación es extrapolable al contexto ecuatoriano, donde el ecosistema de pagos interoperables incorpora entidades de diferente perfil técnico, capacidad de ciberdefensa y gobernanza interna.

Asimismo, el régimen de protección de datos personales en Ecuador, aunque vigente normativamente, aún se encuentra en etapa de implementación operativa. Si bien la Ley Orgánica de Protección de Datos Personales y su Reglamento establecen principios, obligaciones de seguridad y procedimientos ante vulneraciones, no existen —aún— protocolos específicos y efectivos frente a casos de suplantación de identidad o fraude por ingeniería social en entornos digitales. Esto contrasta con la LGPD de Brasil, que impone obligaciones más directas y mecanismos de reparación inmediata en caso de incidentes, como ha sido evidente en el reciente ciberataque al sistema PIX.



[3]Es decir, la capacidad de los sistemas de pago para permitir la transferencia de fondos entre distintas entidades financieras o tecnológicas—bancos, cooperativas, billeteras electrónicas o fintechs—sin restricciones de red o proveedor, a través de estándares técnicos públicos, accesibles y supervisados.

Desde una perspectiva de gobernanza regulatoria, Ecuador enfrenta el reto de articular las competencias del BCE, la Junta de Política y Regulación Financiera y Monetaria y las Superintendencias, para que exista una visión coordinada sobre los riesgos del sistema interoperable. A diferencia de Brasil, donde el BCB concentra funciones de regulación, operación y supervisión del sistema de pagos, en Ecuador el esquema institucional puede diluir la trazabilidad de responsabilidades en caso de fallas.

En suma, el modelo ecuatoriano presenta un riesgo similar al del ecosistema PIX, agravado por la falta de mecanismos correctivos inmediatos y por la ausencia de obligaciones de cobertura frente a incidentes sistémicos. La emulación tecnológica sin adaptación normativa puede producir efectos adversos para la confianza, la estabilidad y la seguridad jurídica del sistema de pagos.

5. Cobertura de riesgo por fraude en sistemas de pagos inmediatos: ¿es necesaria una obligación normativa?

La creciente sofisticación de los delitos informáticos, particularmente en entornos de pagos instantáneos e interoperables, ha reconfigurado las exigencias regulatorias en torno al principio de responsabilidad financiera y protección al usuario. La necesidad de establecer mecanismos obligatorios de cobertura de riesgos por fraude electrónico se vuelve inevitable frente a incidentes de alto impacto.

En el caso de PIX, la arquitectura regulatoria brasileña contempla un Mecanismo Especial de Devolución (MED) para disputas transaccionales, el cual permitió ejecutar devoluciones parciales a víctimas, facilitando la reparación económica. Además, el Banco Central de Brasil propuso, tras el ataque de junio de 2025, un paquete normativo que incluye auditorías reforzadas para Fintech, y responsabilidad subsidiaria de los nodos por fallas internas.

En el Ecuador, la Resolución No. BCE-GG-008-2025 no exige actualmente la contratación de seguros ni establece un esquema de compensación automática en caso de fraude, más allá de la responsabilidad que pudiera imputarse según las normas civiles o administrativas. Tampoco la Ley Fintech o su reglamento han previsto de manera expresa mecanismos de aseguramiento de pérdidas derivadas de fallas tecnológicas, intrusiones o ingeniería social, a pesar de haber reconocido expresamente el principio de protección al consumidor digital.

La normativa aplicable a instituciones financieras autorizadas exige que éstas implementen planes de continuidad de negocios, políticas de gestión de riesgos tecnológicos y sistemas de detección de fraudes, pero no obliga a mecanismos de restitución inmediata ni coberturas contractuales por eventos operativos.

La inclusión de un requisito normativo de cobertura contra fraudes ya sea mediante seguros o fondos de compensación, puede operar bajo una lógica de regulación proporcional: mayores exigencias para participantes con alto volumen de operaciones o con mayor exposición operativa.

Esta previsión permitiría blindar a los usuarios frente a vacíos de responsabilidad, así como fortalecer la estabilidad del sistema, disuadir conductas negligentes y asegurar una compensación efectiva sin necesidad de judicialización.

Adicionalmente, una arquitectura de gobernanza clara sobre quién asume el riesgo residual —cuando no se puede identificar un culpable directo— resulta indispensable para mantener la confianza en el sistema. La posibilidad de implementar un mecanismo análogo al MED brasileño en el entorno ecuatoriano debería evaluarse como prioridad.

En conclusión, la ausencia de un régimen legal de cobertura de riesgo por fraude electrónico en el Ecuador representa una debilidad estructural del actual esquema de pagos interoperables. La experiencia de PIX demuestra que este tipo de medidas no son opcionales, sino parte esencial del diseño jurídico de un sistema confiable, resiliente y centrado en el usuario.

6. Conclusiones y recomendaciones

La adopción de sistemas de pagos interoperables en tiempo real constituye un hito en la transformación digital del sistema financiero ecuatoriano. Sin embargo, este avance, impulsado por la Junta de Política y Regulación Financiera y Monetaria y el Banco Central del Ecuador -mediante el Sistema Integrador de Pagos (SIP) y la Red de Pagos Instantáneos (RPI)- ha generado nuevos desafíos jurídicos que no pueden ser subestimados.

La experiencia reciente del sistema PIX en Brasil, particularmente el ciberataque de junio de 2025, demuestra que incluso los ecosistemas más sofisticados son vulnerables ante fallas estructurales y brechas de seguridad, deficiencias de supervisión y ausencia de cobertura financiera frente a incidentes masivos.

En el caso ecuatoriano, el marco normativo vigente establece una base habilitante adecuada, pero aún incompleta. No se contemplan mecanismos automáticos de reversión de fondos, ni obligaciones de contratación de seguros o fondos compensatorios para enfrentar pérdidas por fraude. Tampoco se ha definido con precisión un régimen de responsabilidad compartida o solidaria entre los distintos participantes del sistema.

Con base en el análisis técnico y comparado, se plantean las siguientes recomendaciones:

1. **Incorporar una normativa específica sobre responsabilidad en arquitectura interoperable,** que delimite deberes de vigilancia, diligencia y compensación frente a eventos de fraude electrónico.

2. **Establecer la obligación regulatoria de cobertura de riesgos operativos,** ya sea mediante seguros obligatorios, fondos de garantía sectoriales o mecanismos de reaseguro, especialmente para entidades con alto volumen o nivel de exposición.

3. **Diseñar un mecanismo especial de reversión** similar al MED brasileño, que permita a las víctimas de fraude electrónico obtener una reparación expedita y sin judicialización.

4. **Fortalecer la supervisión técnica de los nodos participantes,** especialmente Fintech, cooperativas y entidades con menores capacidades tecnológicas, a través de auditorías periódicas y estándares mínimos de ciberseguridad.

5. **Promover una gobernanza regulatoria coordinada** que permita actuar con agilidad ante amenazas sistémicas y defina con claridad los canales de atribución de responsabilidad.

6. **Incluir en los contratos entre participantes del SIP cláusulas obligatorias sobre gestión de incidentes, reportes y protocolos de reversión,** bajo esquemas de responsabilidad cruzada y penalidades por incumplimiento.

7. **Armonizar estas reformas con la Ley Orgánica de Protección de Datos Personales,** a fin de garantizar el tratamiento seguro y legal de la información sensible utilizada para autenticar y validar operaciones en tiempo real.

En definitiva, el sistema de pagos interoperables debe concebirse no solo como una innovación técnica o financiera, sino como una infraestructura crítica que demanda una protección jurídica especial. Incorporar principios de responsabilidad, resiliencia y cobertura no es una opción política, sino una necesidad normativa urgente si se desea consolidar la confianza del usuario y preservar la estabilidad del sistema financiero frente a amenazas cada vez más complejas.

60 AÑOS

asobanca
Asociación de Bancos del Ecuador

VII **Jornadas de** Seguridad Bancaria

www.asobanca.org.ec