UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE OTRAS MODALIDADES DE ESTUDIO

CARRERA DE DERECHO EN LINEA

"EVALUACIÓN JURÍDICA DE RIESGOS Y VULNERABILIDADES EN LA PROTECCIÓN DE DATOS EN INSTITUCIONES FINANCIERAS DEL ECUADOR BAJO LA LEY ORGÁNICA DE PROTECCIÓN DATOS PERSONALES"

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

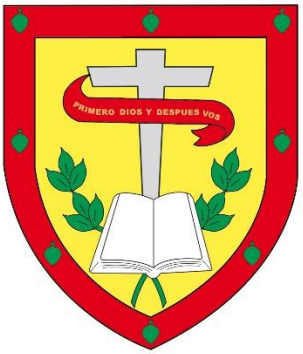
AUTOR: MOSCOSO LEÓN JUAN DIEGO

DIRECTOR: ABG. DARQUEA CARRASCO PEDRO DAVID, MGS.

CUENCA – ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE OTRAS MODALIDADES EN ESTUDIO

CARRERA DE DERECHO EN LÍNEA

"EVALUACIÓN JURÍDICA DE RIESGOS Y VULNERABILIDADES EN LA PROTECCIÓN DE DATOS EN INSTITUCIONES FINANCIERAS DEL ECUADOR BAJO LA LEY ORGÁNICA DE PROTECCIÓN DATOS PERSONALES"

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

AUTOR: MOSCOSO LEÓN JUAN DIEGO

DIRECTOR: AB. DARQUEA CARRASCO PEDRO DAVID, MGS.

CUENCA-ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO

“Evaluación jurídica de riesgos y vulnerabilidades en la protección de datos en instituciones financieras del Ecuador bajo la Ley Orgánica de Protección Datos Personales”

Juan Diego Moscoso León

Universidad Católica de Cuenca

Unidad de titulación

Abg. Pedro David Darquea Carrasco, Mgs.

03 de junio de 2025

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Yo, **Juan Diego Moscoso León,** portador de la cédula de ciudadanía Nº **0105788756**. Declaro ser el autor de la obra: **"Evaluación jurídica de riesgos y vulnerabilidades en la protección de datos en instituciones financieras del Ecuador bajo la Ley Orgánica de Protección Datos Personales",** sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, junio de 2025

JUAN DIEGO MOSCOSO LEON

Firmado digitalmente por JUAN DIEGO MOSCOSO LEON
DN: cn=JUAN DIEGO MOSCOSO LEON, o=SECURITY DATA S.A. 2, ou=ENTIDAD DE CERTIFICACION DE INFORMACION, email=jdmoscoso217@hotmail.com
Fecha: 2025.05.30 22:27:26 -05'00'

……..

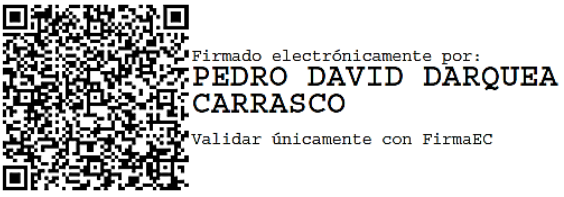
Juan Diego Moscoso León

CERTIFICACIÓN

Yo, **Pedro David Darquea Carrasco**, certifico que el artículo titulado **"Evaluación jurídica de riesgos y vulnerabilidades en la protección de datos en instituciones financieras del Ecuador bajo la Ley Orgánica de Protección Datos Personales",** fue desarrollado por **Juan Diego Moscoso León**, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la Universidad Católica de Cuenca.

Debido a que es una investigación particular con el propósito de cumplir un requisito previo a la obtención del **TITULO DE ABOGADO.**

Cuenca, junio de 2025



Abg. Pedro David Darquea Carrasco, Mgs.
Tutor
UNIVERSIDAD CATÓLICA DE CUENCA

AGRADECIMIENTO

A la Universidad Católica de Cuenca, por brindarme las herramientas académicas necesarias para mi formación profesional, y de manera especial a los docentes de la carrera de Derecho de la Unidad Académica de Otras Modalidades de Estudio, por su dedicación y compromiso en cada etapa del proceso formativo.

Expreso también mi reconocimiento al Dr. Juan Fernando Valarezo y al Dr. David Vásquez, quienes desde el inicio de mi formación supieron guiarme con generosidad, exigencia y claridad. Su acompañamiento y orientación constante fueron fundamentales para mantener la motivación y alcanzar este objetivo profesional.

DEDICATORIA

A mi esposa, por su amor incondicional y su constante compañía. Gracias por ser mi sostén en los momentos de incertidumbre y por creer en mí incluso cuando yo dudaba. Este logro también es tuyo.

A mi hija, por entender que papá necesitaba tiempo para estudiar, y por ser mi principal fuente de inspiración para alcanzar este objetivo. Tu presencia me dio la fuerza y el propósito que necesitaba para seguir adelante.

RESUMEN

La digitalización en el sector financiero ecuatoriano ha incrementado los riesgos en la protección de datos personales, evidenciados en ciberataques y deficiencias en la aplicación de la Ley Orgánica de Protección de Datos Personales (LOPDP), en donde persisten brechas en ciberseguridad, infraestructura y formación del personal, afectando la salvaguarda de la información sensible del ámbito financiero. La presente investigación tiene como finalidad evaluar los riesgos y vulnerabilidades en la protección de datos en instituciones financieras desde la vigencia de la LOPDP, con el fin de evaluar su nivel de implementación y proponer medidas que aseguren la protección integral de los derechos constitucionales de los ciudadanos sobre sus datos. El estudio fue realizado aplicando un enfoque cualitativo mediante la revisión de normativa, jurisprudencia y doctrina, además de un análisis de Derecho comparado. Como resultado se evidencia que existen brechas en la aplicación de medidas de seguridad, reflejadas en la exposición de datos y limitaciones en el cumplimiento normativo. De ello se deriva la urgencia de optimizar los procedimientos de fiscalización vigentes y la respectiva actualización tecnológica para garantizar una protección efectiva. Como conclusión se recomienda el planteamiento de estrategias como auditorías obligatorias, modernización tecnológica y educación digital a efectos de reforzar la integridad y confidencialidad de los datos en el sector financiero ecuatoriano.

Palabras clave: Protección de datos, seguridad informática, derecho informático, tecnología de la información, riesgo

ABSTRACT

Digitalization in the Ecuadorian financial sector has increased risks to personal data protection, as evidenced by cyber-attacks and deficiencies in the enforcement of the Organic Law for the Protection of Personal Data (LOPDP, by its Spanish acronym). Persistent gaps in cybersecurity, infrastructure, and staff training comprise safeguarding sensitive information within the financial sector. This research aims to evaluate the risks and vulnerabilities in data protection in financial institutions since the LOPDP came into force, to assess its implementation level, and to propose measures to ensure the comprehensive protection of citizens' constitutional rights over their data. The study employed a qualitative approach through the review of regulations, jurisprudence, and legal doctrine, as well as a comparative law analysis. The findings reveal gaps in the implementation of security measures, which are reflected in the exposure of sensitive data and limitations in regulatory compliance. Therefore, there is an urgent need to optimize existing control procedures and the respective technological updates to ensure adequate protection. In conclusion, it is recommended that strategies such as mandatory audits, technological modernization, and digital education be implemented to strengthen data integrity and confidentiality in the Ecuadorian financial sector.

Keywords: Data protection, computer security, computer law, information technology, risk

Introducción

En el mundo actual, especialmente digital en donde cada transacción o búsqueda deja una huella, el resguardo de los datos personales se ha transformado en una necesidad obligatoria. El sector financiero, pilar de la economía digital, administra recursos y además historiales de crédito y patrimonio de una población considerable, convirtiéndolo en un blanco permanente de ataques cibernéticos, filtraciones en masa y fraudes que en solo unos segundos pueden poner en riesgo la estabilidad de un individuo o una entidad.

Es así como en 2021, Ecuador tomó conciencia de esta situación y promulgó la Ley Orgánica de Protección de Datos personales (en adelante LOPDP), un marco regulatorio creado para asegurar la seguridad y la privacidad en la era digital.

Sin embargo, su implementación se topa con barreras estructurales: recursos tecnológicos anticuados, carencias en ciberseguridad y una brecha entre el acatamiento de las regulaciones y la realidad operativa de las instituciones financieras.

Las cifras son claras, según la Superintendencia de Bancos (en adelante SB) en un informe del 2023 menciona que en un solo año se reportaron cuatro mil incidentes de seguridad generando pérdidas superiores a 12 millones de dólares. Más alarmante aún el 35% de las instituciones presentaba deficiencias en sus protocolos de protección de datos, mientras que los intentos de ciberataques crecieron en un 30%; detrás de estos números hay ciudadanos que ven vulnerada su privacidad, empresas que sufren daños reputacionales y un sistema financiero que enfrenta riesgos cada vez más complejos.

De cara a este panorama, el ordenamiento jurídico ecuatoriano ya contempla herramientas específicas para mitigar los riesgos descritos, la LOPDP, establece en sus artículos 33 a 36 la obligación de efectuar evaluaciones de impacto antes de todo tratamiento

de datos críticos, mientras que el Código Orgánico Monetario y Financiero (en adelante COMF) exige a las entidades la gestión integral de riesgos operacionales, incluida la seguridad de la información detallada en su art. 165 (COMF, 2014) No obstante, reportes conjuntos de la SB y la Superintendencia de Protección de Datos Personales (en adelante SPDP) muestran que solo el 38% de las instituciones ha completado las evaluaciones de impacto y que la notificación de incidentes sigue siendo dispareja en su aplicación cotidiana dentro del sistema financiero nacional. (SB, 2023)

En un esfuerzo por reducir esta brecha, Ecuador expidió el reglamento general a la LOPDP, que si bien se inspira en los estándares del Reglamento General de Protección de Datos de la Unión Europea (en adelante RGPD) se adapta al contexto ecuatoriano en principios como la protección de datos desde el diseño y la responsabilidad proactiva.

Por otro lado, replicar modelos exitosos no garantiza su efectividad si no se implementan con estrategias adaptadas a la realidad local. A pesar de que la LOPDP establece requisitos como auditorías periódicas, protocolos de seguridad y supervisión continua, su aplicación práctica enfrenta obstáculos estructurales.

Para ello se formula la pregunta crítica que menciona: ¿de qué manera un marco legal avanzado puede lograr sus metas si las entidades financieras no poseen infraestructura tecnológica apropiada ni personal debidamente formado?

El objetivo principal de este estudio es analizar los riesgos sistémicos y vulnerabilidades en la salvaguarda de la información personal en el sector financiero de Ecuador después de la implementación de la LOPDP que, a través de un análisis crítico de su nivel de implementación, se pretende detectar fallos operativos y sugerir modificaciones normativas y técnicas que garanticen la salvaguarda eficaz de los derechos esenciales de los

propietarios de datos.

Desde una perspectiva metodológica, la investigación se basa en un enfoque cualitativo fundamentado en el examen sistemático de literatura especializada como doctrina, informes regulatorios y jurisprudencia; además de un estudio comparativo de modelos internacionales RGPD, LGPD; y la valoración de casos representativos de infracciones de datos que han ocurrido en Ecuador, este enfoque triple facilitará el contraste entre el marco teórico y la realidad operativa del sistema financiero nacional.

Los datos iniciales revelan que para lograr fortalecer la LOPDP de manera efectiva, es indispensable que se lleven a cabo varias intervenciones en coordinación con distintos frentes.

Para comenzar, es fundamental que se revise y modernice el marco normativo, ya que existen vacíos en su regulación que es necesario abordarlos, de manera especial en lo que respecta a las áreas emergentes como la tokenización de activos y también el uso de IA en cuanto a los datos financieros.

En un segundo plano, en lo relacionado con la tecnología, es emergente la adopción de ciertas medidas de seguridad avanzada como pueden ser los mecanismos de autenticación multifactorial para lograr reducir los riesgos de acceso no autorizado al máximo posible. En última instancia, en el contexto institucional debe considerarse prioritario el fortalecimiento de las capacidades que tiene actualmente de SPDP, esto puede darse a través de implementación de auditorías que sean de manera recurrente y obligatoria; además de mantener un régimen sancionador para evaluar el cumplimento efectivo de dicha normativa.

Es únicamente mediante esta estrategia integral que se podrá construir un ambiente financiero digital que logre ser seguro, para mantener la armonía dentro de los procesos nacionales, que, a su vez, estén alineados con los estándares internacionales de protección de

datos y, primordialmente, poder recuperar la confianza de los ciudadanos cuanto al manejo de su información personal que mantienen en su custodio las instituciones financieras.

A partir de lo expuesto, el artículo está estructurado en cuatro secciones, primero se exponen los fundamentos jurídicos de la protección de datos; luego se identifican los riesgos concretos que afectan a la banca ecuatoriana, posteriormente, se presentan los hallazgos empíricos y finalmente, se formulan recomendaciones orientadas a fortalecer la ciberresiliencia del sistema financiero.

Desarrollo

Fundamentos generales de la protección de datos personales

El origen del proceso histórico y legal de protección de datos personales se remonta a Alemania específicamente en Hesse en donde el nombrado jurista Spiros Simitis realizó un trabajo revolucionario con la creación de la Ley de Protección de Datos del Estado de Hesse, en la cual no se entendía a la protección de datos desde una dimensión técnica sino más bien como una salvaguarda únicamente de los derechos esenciales de las personas en lo que respecta a su información personal. En este sentido Barrio (2024), menciona que esta visión más enfocada en las personas logró establecer las bases para el reconocimiento a escala de la protección de datos y que este se convierta en un derecho independiente en distintos sistemas legales, entre los que se incluyen el marco legal de la Unión Europea y también la Constitución Española.

En este mismo sentido, es necesario indicar que, mucho más allá de ser vista como una medida de seguridad, la protección de datos significa una garantía de que cada persona puede mantener el control sobre su información personal, pues principalmente se encuentra centrado en que esta garantía del manejo de datos se lleve a cabo teniendo en cuenta legalidad,

transparencia y seguridad. (Barrio, 2024)

Enfocándonos en el contexto ecuatoriano, este derecho ha logrado establecer un estatus constitucional, además de un desarrollo normativo específico con la implementación de la LOPDP.

Según el análisis de Lanas y Cárdenas (2023), la LOPDP se encarga de la regulación detallada tanto de los procedimientos como de la recopilación, almacenamiento y tratamiento de la información de los datos en el sector público y privado.

Actualmente, dentro del marco legal, vemos que la protección de la información personal se extiende a múltiples ámbitos los cuales van más allá de únicamente la identificación personal pues abarca un conjunto de información en la que se incluyen desde los componentes más básicos como son el nombre y el número de cédula hasta ciertas categorías que representan una alta vulnerabilidad como pueden ser los registros biométricos y los datos financieros, además de rastreos digitales, e inclusive direcciones IP y huellas dactilares.

En este sentido Ordoñez (2017), advierte que una falta de regulación sólida deja en exposición total a la privacidad de los ciudadanos, además que debilita su habilidad para lograr auto determinarse en los entornos digitales.

Este tema se ve intensificado debido a la época en la cual nos encontramos, en donde la hiperconectividad en la digitalización de servicios se ve envuelta constantemente con amenazas de filtración y también ante la posible manipulación de los datos, lo cual transforma a cada rastreo digital en un territorio muy susceptible, el cual necesita un sustento legal, completo y activo.

Es así que, la legislación de Ecuador ha logrado establecer un conjunto de principios rectores que establecen un verdadero estatuto legal en lo que respecta a la administración de

datos personales. Entre los cuales se encuentran el principio de licitud en cuanto al manejo de información, además de la autenticidad y la actualización de la información; también se menciona la necesidad de crear las medidas de seguridad pertinentes que logren evitar estos accesos no permitidos, en atención al principio de licitud que consta en el artículo 10 de la LOPDP. Con ello, se pretende proteger a los propietarios de los datos y definir un esquema claro de obligaciones para las entidades responsables de su administración.

El Tribunal Constitucional de Ecuador ha fortalecido el derecho a la salvaguarda de la información personal mediante precedentes jurídicos. La Resolución No. 2064-14-EP/21 expande conceptualmente la comprensión de los datos personales al determinar que esta categoría incluye cualquier información que permita identificar a una persona, sin importar su medio físico o digital. Adicionalmente, la resolución establece un aspecto esencial en relación al consentimiento para el tratamiento de datos, indicando que este debe ser libre, específico, informado e inequívoco, lo que reconoce la autodeterminación informativa como un principio fundamental de la LOPDP.

El reconocimiento judicial de la salvaguarda de la información personal va más allá de la simple formalidad jurídica y se fortalece como un derecho esencial que robustece al ciudadano en la era digital. Como indica Barrio (2024), este principio concede a cada persona la facultad de administrar su información personal con total independencia, lo que conlleva determinar estratégicamente quién tiene acceso a sus datos, con qué fines y bajo qué circunstancias, e incluso anular dicho permiso en cualquier instante, así se demuestra que, más allá de la presencia de marcos regulatorios, la auténtica eficacia de este derecho reside en su implementación práctica y, principalmente, en el grado de conciencia social acerca de los derechos digitales, convirtiendo la salvaguarda de datos de un concepto teórico en una realidad

palpable de empoderamiento ciudadano.

Así, la LOPDP se manifiesta como un recurso fundamental el cual está en manos de la ciudadanía y de esta manera proporciona a las personas los recursos esenciales para la administración de su información personal.

En este contexto, Ordoñez (2017) manifiesta que dentro de los derechos que comprenden el acceso a la información tenemos por un lado, el derecho de acceso, el cual de cierta manera facilita la identificación de los datos que se han recolectado y para qué serán utilizados; además nos menciona el derecho de rectificación, el mismo que permite se corrija la información incorrecta; y el derecho de supresión a través del cual las personas que lo requieran pueden pedir la suspensión de sus datos cuando consideren que su uso es inapropiado o innecesario.

Además, se reconoce el derecho de oposición, que permite a los titulares rechazar la utilización de sus datos en ciertas situaciones; y el derecho a la portabilidad, que les facilita el intercambio de sus datos entre distintos proveedores de servicios; estas disposiciones buscan generar un marco de defensa, el mismo que anhela asegurar un trato equitativo de la información personal y establecer un balance en lo que respecta a protección de privacidad y el uso legítimo de los datos en los entornos digitales.

En el diseño de la LOPDP, el primer nivel de autoridad sobre la información recae en el propio titular, pues los artículos 13 a 18 reconocen un haz de derechos que le permite acceder, rectificar, actualizar, suprimir, oponerse y portar sus datos. Es decir que la autodeterminación informativa deja de ser un postulado teórico y se materializa en acciones concretas con las que cualquier ciudadano puede constatar la veracidad de los registros, exigir su corrección o su eliminación cuando el tratamiento resulte improcedente.

El sistema jurídico de Ecuador establece ciertas responsabilidades específicas para quienes gestionan los datos personales, cuya tutela se encuentra en manos tanto de las entidades gubernamentales como de las empresas. Se reconoce como una de las más destacadas a la exigencia de validación previa que deben autorizar los ciudadanos para el acceso a su información a través de mecanismos pertinentes. Además de ello, es necesario que se implementen medidas de seguridad reforzadas, las cuales podrían centrarse en buscar la manera de anticipar los accesos no autorizados y a su vez asegurar la integridad de los datos almacenados.

Con el fin de fortalecer este aspecto, la LOPDP dispone la obligación de contar con un delegado de Protección de Datos en cada una de las instituciones encargadas del manejo de la información, en donde su objetivo principal es llevar a cabo una rigurosa supervisión al acatamiento de las normativas, así como también funcionar como enlace entre la entidad y los titulares de la información conforme a los artículos 48 y 49 de la misma ley. (LOPDP, 2021)

En cuanto al sector financiero se refiere, la seguridad de la información personal se instaura como un requisito de seguridad primordial, tal como lo indica Ordoñez (2017). La información de los clientes de las instituciones financieras, requiere estrictos protocolos de seguridad extremadamente especializados, ya que incluye historiales de crédito y registros de transacciones bancarias, entonces deben ser capaces de reducir cualquier peligro de filtración o mal uso.

Para enfrentar este reto, la LOPDP establece las normas de confidencialidad estrictas y también procedimientos de control muy estrictos y rigurosos que aseguran el manejo correcto de la información delicada; y con este enfoque regulatorio pretende proteger los derechos personales de los clientes, además de convertirse en un componente esencial para la

subsistencia de la integridad y estabilidad del sistema bancario, y lograr disminuir la posible vulnerabilidad de información.

También, es necesario tener en consideración que esta revolución digital actual de la que se habla ha promovido una reconstrucción enérgica en cuanto se refiere al tema de la privacidad, pues logra desafiar los confines convencionales de los sistemas legales nacionales. De esta manera Lanas y Cárdenas (2023) abordan este tema, explicando que las leyes ecuatorianas han reaccionado a este fenómeno con la creación de una estrategia de adaptación normativa, en la cual se incorporan una serie de normas internacionales, las cuales están fundamentadas particularmente en el RGPD europeo, cuyo objetivo final es establecer un sistema de protección integral en un ambiente digital que cada día incrementa su complejidad.

La efectividad real de esta normativa no está únicamente basada en lo que concierne a su estructura técnica, pues también se centra en esta habilidad para crear una cultura legal que supere el simple cumplimiento formal, sino que además fomente un ejercicio consciente y proactivo de los derechos de la protección de la información.

Principales riesgos en la protección de datos personales en el sector financiero ecuatoriano

La digitalización del sistema financiero nacional representa un contexto lleno de retos pues la innovación tecnológica está llena de innumerables desafíos en cuestión de seguridad. Y en este contexto, Guamán et al. (2023) muestran un análisis realmente alarmante, en el mismo que presenta tres factores considerados claves en cuestión de riesgo, como primer punto menciona a la diversidad en la implementación tecnológica entre entidades financieras, además de la desincronización entre el marco normativo y las capacidades operativas reales, y también hace mención al incremento exponencial de las amenazas cibernéticas externas.

La integración de estos tres factores da como resultado varias desigualdades

estructurales en lo que respecta a la salvaguarda de la información y de esta manera también disminuye gradualmente la confianza de todos los usuarios en lo concerniente a la infraestructura digital del sistema financiero nacional.

En lo que respecta al plano normativo, la LOPDP dispone en sus artículos 33 y 36 que toda entidad financiera debe realizar una evaluación de impacto en la protección de datos antes de tratar información sensible y repetirla siempre que cambie la tecnología empleada. (LOPDP, 2021) además, el COMF en su artículo 165 integra el riesgo de seguridad de la información en la gestión integral de riesgos que supervisa la SB. (COMF, 2014)

Además, según la SB (2023), únicamente el 28% de las instituciones financieras disponen de dispositivos especializados en ciberseguridad, lo que sitúa a la mayoría de estas entidades en un estado de vulnerabilidad. Aunque en Europa la puesta en marcha de auditorías obligatorias ha disminuido los incidentes en 40%, en Ecuador la observancia de las normas continúa siendo insuficiente debido a la ausencia de inversión en infraestructura y la escasa vigilancia de las autoridades reguladoras.

Amenazas cibernéticas y su impacto en la banca ecuatoriana

Los ataques digitales configuran hoy uno de los principales riesgos operacionales para la integridad de la información financiera, por lo que Ecuador ha sido blanco de múltiples ataques informáticos dirigidos a entidades bancarias, comprometiendo información financiera crítica y elevando las preocupaciones sobre la protección de datos personales en este ámbito; ya que si bien la digitalización de los servicios financieros ha facilitado transacciones más eficientes y también ha incrementado la superficie de ataque para distintos tipos de ciberdelitos. (Guamán et al., 2023).

Dentro del espectro de amenazas cibernéticas contemporáneas, destacan

particularmente el phishing y la suplantación de identidad, modalidades delictivas que mediante ingeniería social buscan sustraer credenciales bancarias de usuarios desprevenidos.

Según alerta Barrio (2024), los delitos mencionados anteriormente han logrado escalar grados muy preocupantes en cuanto a sofisticación pues integran varios instrumentos de inteligencia artificial, además de un análisis predictivo de comportamiento y con esto logran superar los métodos convencionales de detección y esto resulta preocupante.

En el mismo sentido de alerta, se ve una escalada igualmente delicada en lo que respecta al ransomware, pues mediante esto los actores malintencionados utilizan malware encriptado para lograr de esta manera extraer datos delicados y posteriormente solicitan los llamados rescates financieros por la liberación de esta información. Este tipo de crimen cibernético, de acuerdo con Orellana (2017) va mucho más allá del daño individual que puede causar, para transformarse en un peligro ya sistémico. Esto se debe a que a más del efecto económico directo que causa, también provoca un quiebre operativo en las entidades financieras y de esta manera debilita la fe pública en los sistemas de pago digitales.

Otro de los peligros importantes en este campo son el fraude financiero y el robo de identidad, delitos en los cuales los delincuentes logran acceder a la información personal para luego utilizarla en la realización de transacciones no autorizadas, con lo cual se desencadenan una serie de costos adicionales, pues las instituciones financieras deben implementar medidas de seguridad y a la vez restituir los fondos de los ciudadanos que resultaron víctimas de esta situación. (Orellana, 2017)

En este contexto, es necesario que las instituciones financieras refuercen sus sistemas de seguridad, capaciten a su personal y fomenten la educación digital entre sus clientes para minimizar los riesgos asociados a las amenazas cibernéticas (Guamán et al., 2023). Y de este

modo, la LOPDP establece principios clave para la seguridad de la información y la prevención de su uso indebido. (LOPDP, 2021).

Vulnerabilidades internas y debilidades en las infraestructuras tecnológicas

Además de los ataques externos, muchas de las brechas de seguridad en las instituciones financieras se deben a deficiencias internas. Según la Comisión Económica para América Latina y el Caribe (en adelante CEPAL), la falta de capacitación del personal y la ausencia de políticas robustas de ciberseguridad aumentan significativamente el riesgo de exposición de los datos personales (CEPAL, 2021).

Un estudio de Carvajal (2022) identificó que el 40% de las filtraciones de datos en bancos provienen de errores humanos o accesos indebidos por parte de empleados, lo cual pone en evidencia la necesidad de ejecutar programas de concienciación e instrucción en protección de datos dentro de las entidades financieras. Por lo tanto, el fortalecimiento de infraestructuras tecnológicas se convierte en una prioridad y la inversión en sistemas avanzados de cifrado de datos más la modernización de plataformas digitales y una adecuada colaboración con organismos internacionales especializados en ciberseguridad podría proporcionar herramientas y metodologías eficaces para mitigar las vulnerabilidades identificadas.

Evaluación de casos de ciberataques en instituciones financieras en Ecuador

El sistema financiero ecuatoriano ha enfrentado en los últimos años un incremento exponencial de incidentes de ciberseguridad, evidenciando vulnerabilidades estructurales ante amenazas de la creciente sofisticación técnica, los cuales han generado pérdidas cuantificables en términos lo referente a términos económicos, además han dado lugar a complejas consecuencias jurídicas, particularmente en lo relativo a la responsabilidad por protección de datos personales.

Un caso paradigmático lo constituye el ciberataque sufrido a la Cooperativa Juventud Ecuatoriana Progresista (en adelante Coop. JEP), debido a que en el año 2021, actores no autorizados explotaron vulnerabilidades en los sistemas internos de la entidad, comprometiendo datos sensibles de un número crítico de clientes; esta intrusión permitió el acceso ilícito a información privilegiada sobre cuentas de ahorro, líneas de crédito y movimientos financieros, en clara vulneración de los principios de confidencialidad y seguridad establecidos en la LOPDP. (Coop. JEP, 2023)

Consecuencia de aquello, la cooperativa implementó un plan bastante completo el cual estaba comprendido por el fortalecimiento de la infraestructura tecnológica, la puesta en marcha de sistemas de autenticación de vanguardia, y también distintos programas de formación y capacitación constante para el personal en lo que respecta a la identificación de amenazas a tiempo.

Desde el punto de vista legal, este suceso originó reclamaciones de clientes por infracción a la información personal, lo que generó discusiones acerca de la implementación eficaz de la LOPDP en el sector financiero, es por ello que la SB tomó medidas, demandando informes técnicos y acciones correctivas inmediatas. (SB, 2023).

Otro caso de gran impacto ocurrió en 2019, cuando la empresa Novaestrat involucró la exposición no autorizada de registros personales que superaban los 20 millones de casos documentados, esta filtración masiva reveló datos bancarios, registros civiles y detalles financieros. El problema se originó debido a la ausencia de protocolos de seguridad en los servidores donde se almacenaba la información, pues al estar alojados sin protección en la nube, terceros pudieron acceder sin restricciones. (Instituto Nacional de Ciberseguridad, 2019)

Situación similar se dio en octubre de 2022, cuando el Banco Pichincha fue víctima de

un ciberataque tipo ransomware, afectando gravemente la continuidad de sus servicios financieros. Este ataque fue ejecutado mediante una estrategia de phishing dirigido a empleados, lo que permitió la instalación del ransomware en los sistemas del banco; el resultado fue una caída masiva de los servicios digitales, bloqueando cajeros automáticos y transacciones en línea por lo que millones de clientes se vieron afectados, generando retrasos en pagos y transacciones. (Diálogo Américas, 2022)

Ante esta crisis, el banco implementó protocolos de recuperación, fortaleció su seguridad multicapa y capacitó a su personal sobre prevención de ataques, además, el incidente reavivó la discusión sobre la responsabilidad de las entidades bancarias en la protección de datos financieros y la urgencia de auditorías obligatorias en ciberseguridad (Guamán et al., 2023).

La vulneración de datos personales en el sector financiero ecuatoriano ha sido objeto de análisis judicial en varios casos, como referencia tenemos la Sentencia No. 839-14-EP/21 en la cual la Corte Constitucional fija estándares para armonizar dos garantías constitucionales en tensión, por un lado, la publicidad de actos de interés público y por otro la inviolabilidad de la vida privada. Este criterio se vuelve particularmente determinante al regular qué detalles deben revelarse ante un ciberataque a una entidad financiera, pues exige ponderar caso por caso hasta qué punto la transparencia justifica afectar la esfera personal de clientes o empleados.

Evaluación del cumplimiento normativo y su impacto en la seguridad de los datos

En el contexto internacional, la Unión Europea se destaca como un referente en lo que respecta a protección de datos personales desde la entrada en vigor del RGPD en 2018. Esta normativa es considerada la más avanzada y detallada pues no únicamente está enfocada y

limitada en el establecimiento de sanciones económicas sino que también incorpora el principio de privacidad por diseño que obliga a las empresas a buscar internalizar las medidas se seguridad en cada una de las etapas de su operación. (Barrio, 2024)

El impacto del RGPD ha pasado las fronteras europeas y ha logrado marcar ciertos referentes en varios países de América Latina, entre los cuales Ecuador está incluido, pues esta normativa ha servido de referencia para varias reformas en sus propias leyes (Journal of Economic and Social Science Research, 2024). A pesar de ello, existen investigaciones comparadas en donde se menciona que la implementación efectiva de estos estándares se topa con ciertas barreras que resultan ineludibles, las cuales están originadas por desigualdades económicas, además de diferentes capacidades institucionales e incluso resistencias culturales en lo que respecta al control de datos.

Una gran fortaleza del RGPD es justamente el principio de responsabilidad proactiva, el cual requiere que las compañías cumplan las regulaciones y también lograr evidenciar tal acatamiento mediante procedimientos como auditorías regulares y evaluaciones de impacto en la privacidad. De acuerdo con cifras de Journal of Economic and Social Science Research (2024), ha propiciado que más del 60% de las entidades en Europa implementen herramientas tecnológicas enfocadas en la administración de riesgos, evidenciando un cambio en cuanto a la estructura de los modelos de gobierno más abiertos.

Pese al notable avance normativo, el RGPD aún plantea obstáculos importantes en su ejecución práctica particularmente en lo las pequeñas y medianas empresas (PYMES), pues existen datos recientes que indican que alrededor del 40% de estas compañías no poseen los medios financieros ni técnicos necesarios para nombrar un delegado de Protección de Datos (en adelante DPO), a pesar de ser una figura muy importante en el marco regulatorio europeo

(Journal of Economic and Social Science Research, 2024)

La diferencia en los recursos para cumplir con la normativa expone una tensión legal que nos lleva a preguntarnos si puede una regulación establecida para grandes corporaciones adaptarse a entornos empresariales más tradicionales o menores sin generar grandes desbalances

Dicho esto, podemos ver que, aunque el RGPD ha incrementado los estándares de seguridad de la información a escala mundial, de la misma manera ha recibido una serie de críticas debido a la burocracia excesiva y los altos costos que puede llegar a implicar su implementación, especialmente en sectores con márgenes operativos mucho más reducidos.

Como complemento, El Reglamento de Resiliencia Operativa Digital (en adelante DORA), establecido en 2022, también ha logrado fortalecer de manera considerable el marco normativo europeo sobre todo en lo que respecta al mercado financiero, pues ha puesto especial atención a aquellas interacciones sistémicas entre las entidades bancarias, los proveedores de servicios en la nube y también otros participantes de este ámbito (Barrio, 2024). Este Reglamento logra constituir demandas muy novedosas como son la ejecución regular de exámenes de estrés cibernético, también el control directo de proveedores de tecnología a través de auditorías obligatorias, así como la fijación de tiempos rigurosos no superiores a dos horas para la comunicación de incidentes pertinentes.

Estos procedimientos evidencian que la transformación conceptual en lo que respecta a la salvaguarda de los datos, donde el foco ya no está limitado en la prevención y vulnerabilidades; sino que también busca asegurar estas capacidades institucionales sólidas para lograr reaccionar de manera eficiente ante ciberataques. Además, el reglamento exige un enfoque mucho más proactivo el cual comprende la interrelación de los riesgos digitales en el

sistema financiero y define varios criterios de resistencia operativa que nunca antes se han visto en la legislación.

Tal como se evidencia, a pesar de que el RGPD, ha tenido un enorme aporte en lo que respecta a la promoción de estándares de transparencia y cumplimiento normativo, también ha recibido críticas significativas en relación a la efectividad de sus requerimientos para actores económicos con ciertas capacidades limitadas restringidas. Pues al estar diseñada principalmente para empresas o corporaciones grandes es inevitable que presente varios retos sobre todo en lo operativo y en la puesta en marcha de los sistemas de riesgo más sofisticados. (Cámara de Fintech Ecuador, 2023).

Latinoamérica frente a la protección de datos: avances normativos y brechas en la implementación

La implementación de regulaciones como el RGPD en países fuera de la UE enfrenta desafíos estructurales. Por ejemplo, Cámara de Fintech Ecuador. (2023) sostiene que la extraterritorialidad del RGPD genera tensiones en naciones con sistemas legales fragmentados, ya que impone estándares diseñados para economías consolidadas. En Ecuador, esto se refleja en el 60% de las entidades financieras.

La realidad normativa latinoamericana carece de asesoría legal especializada para interpretar cláusulas de transferencia internacional de datos, lo que limita su capacidad de cumplimiento. Este hallazgo cuestiona la visión de Barrio (2024), quien minimiza los efectos adversos de la adopción acrítica de modelos europeos; existe un contraste con el modelo europeo, caracterizado por su coherencia supranacional, pues mientras la Unión Europea cuenta con un marco jurídico unificado en materia de protección de datos, la región latinoamericana enfrenta significativos desafíos en la armonización regulatoria, lo cual se

manifiesta claramente en los casos de Brasil y Argentina, países que pese a haber modernizado su legislación adoptando la Lei Geral de Proteção de Dados (en adelante LGPD) y actualizando la Ley 25.326 respectivamente mantienen importantes divergencias tanto en su implementación práctica como en sus mecanismos de supervisión (Barrio, 2024).

Estas diferencias dificultan la creación de un estándar regional común y generan inseguridad jurídica para actores transnacionales que operan en múltiples jurisdicciones.

El caso de Brasil ilustra una notable singularidad regulatoria debido a que mientras la LGPD incorpora disposiciones avanzadas como el derecho al olvido y el requisito de consentimiento expreso, su implementación efectiva enfrenta obstáculos significativos, pues según datos de la Asociación Latinoamericana de Ciberseguridad (2023), aproximadamente el 70% de las organizaciones en Brasil aún no realizan evaluaciones sistemáticas de impacto en la privacidad, pese a ser un mandato legal. Esta brecha entre el marco normativo y su aplicación práctica según lo explica Barrio (2024), revela los desafíos estructurales que persisten en la región, particularmente en lo relativo a capacidades técnicas y cultura de cumplimiento.

De la misma manera, la situación en Argentina presenta matices distintos, pero igualmente complejos, puesto que el acelerado desarrollo del ecosistema fintech ha superado la capacidad regulatoria, con numerosas empresas implementando soluciones blockchain sin incorporar protocolos robustos de cifrado o gestión de identidad digital. Esta situación genera vulnerabilidades críticas que podrían derivar por un lado en fraudes por suplantación de identidad, además de alteración maliciosa de contratos inteligentes, y también en exposiciones masivas de datos sensibles. Tales riesgos, documentados en recientes informes del Banco Central de Argentina (2024), evidencian la urgencia de actualizar los marcos de supervisión para tecnologías emergentes.

La ausencia de una regulación regional armonizada en América Latina produce inconsistencias jurídicas significativas. Un claro ejemplo se observa en las diferencias entre México y Chile, en donde el primero requiere autorización previa para transferir datos fuera de sus fronteras, mientras que el segundo permite dichas transferencias siempre que el destinatario ofrezca niveles de protección equivalentes. Esta falta de estandarización dificulta el funcionamiento de las plataformas digitales con operaciones regionales, especialmente en áreas como el comercio electrónico y los servicios financieros, generando complicaciones tanto para las empresas como para los usuarios finales.

Las plataformas de crowdfunding enfrentan desafíos particulares en Latinoamérica, donde deben adaptar sus operaciones a marcos regulatorios divergentes en países como Colombia, Perú y Ecuador. Esta disparidad normativa eleva sustancialmente los costos de operación y, paralelamente, complica la implementación de mecanismos efectivos contra delitos digitales transfronterizos, particularmente en casos de lavado de activos mediante criptomonedas. La actual fragmentación legislativa regional, lejos de ser un problema meramente técnico, impacta directamente en dos dimensiones críticas: por un lado, debilita las garantías de protección de datos personales; por otro, frena el potencial innovador y el crecimiento sostenible de la economía digital en la región.

El ordenamiento jurídico ecuatoriano dio un salto cualitativo con la implementación de la LOPDP en 2021, norma que incorporó estándares contemporáneos como el derecho a la portabilidad de datos, el principio de transparencia algorítmica y la creación de una autoridad de control especializada: la SPDP. Sin embargo, persisten lagunas regulatorias significativas, particularmente en materia de tokenización de activos financieros, tecnología ampliamente adoptada por la banca local para garantizar la seguridad en transacciones digitales, pero que

carece de regulación específica en la LOPDP. Esta omisión evidencia un desafío estructural pues, la velocidad del desarrollo tecnológico supera la capacidad de respuesta normativa.

En contraste, Castro et al. (2023) cuestionan el paradigma jurídico actual, centrado excesivamente en la protección individual de la privacidad, según su análisis, este enfoque presenta una limitación estructural debido a que pasa por alto fenómenos macro como la creciente concentración de poder en manos de conglomerados tecnológicos transnacionales, quienes determinan de facto los estándares globales de tratamiento de datos. Este análisis es relevante para Ecuador, donde el 80% de las plataformas digitales utilizadas por bancos locales son proveídas por empresas extranjeras sujetas a jurisdicciones con estándares divergentes (SPDP, 2023). Así, mientras Barrio (2024) enfatiza la adaptación normativa, Zuboff revela un vacío estratégico: la dependencia tecnológica socava la soberanía de datos. Esta lógica confirma la advertencia de que la extracción masiva de información personal se ha convertido en el insumo principal de un nuevo régimen económico de vigilancia. (Zuboff, 2021)

Por otro lado, Castro et al. (2023) proponen que las regulaciones deberían priorizar la educación del usuario como mecanismo de protección. Es así que, en Ecuador, solo el 35% de los clientes bancarios comprende sus derechos bajo la LOPDP, según una encuesta de la Defensoría del Pueblo (2023), lo que sugiere que la eficacia de la ley depende de su cumplimiento institucional y de la alfabetización digital ciudadana; esta perspectiva amplía el enfoque de Barrio Andrés, centrado en auditorías, al incorporar la corresponsabilidad social en la protección de datos.

Propuesta de estrategias para fortalecer la seguridad de los datos en el sector financiero

La protección de datos en el sector financiero ecuatoriano demanda un enfoque integral que combine tecnología, formación y cooperación institucional. Como señalan Paredes y

Salazar (2021), la implementación de tecnologías de encriptación avanzada, como el estándar de cifrado avanzado AES-256, reduce hasta en un 60% las vulnerabilidades en transacciones digitales, al garantizar la integridad y confidencialidad de la información. Este avance técnico se alinea con el artículo 37 de la LOPDP, que exige a las entidades financieras adoptar medidas tecnológicas adecuadas.

Así pues, para maximizar su eficacia, estas herramientas deben complementarse con sistemas de autenticación multifactorial como son la biometría o tokens dinámicos, tal como recomienda el RGPD, lo que mitiga riesgos de acceso no autorizado y además proyecta al sistema bancario ecuatoriano como un entorno seguro ante inversionistas internacionales.

Sin embargo, la tecnología por sí sola no basta si no se aborda el factor humano, principal eslabón débil según González y Andrade (2020), quienes identifican que el 65% de las brechas de seguridad se originan en errores del personal, como el manejo negligente de contraseñas. En este contexto el artículo 42 de la LOPDP establece la obligatoriedad de capacitar a los empleados en protección de datos, pero es imperativo ir más allá mediante programas prácticos. Por ejemplo, simulacros de phishing, desarrollados en colaboración con organismos como la CEPAL, permitirían evaluar respuestas ante amenazas reales y certificar competencias. Esta formación continua reduciría incidentes y fomentaría una cultura organizacional proactiva, donde cada colaborador actúe como un agente de seguridad.

La modernización de infraestructuras tecnológicas en entidades regionales, muchas veces limitadas por recursos económicos, requiere un esfuerzo colaborativo. Maldonado y Vélez (2022) destacan que la cooperación público-privada es clave para superar estas barreras. Es así que el artículo 15 de la LOPDP ya obliga a reportar incidentes a la SPDP, pero se propone crear un fondo mixto financiado por el Estado y la banca privada; el cual podría destinarse a la

adopción de herramientas como inteligencia artificial predictiva, capaz de detectar patrones anómalos en tiempo real, o a la migración de servidores obsoletos a plataformas en la nube con cifrado integral, con el objeto de reducir la dependencia de proveedores extranjeros, fortaleciendo la potencia tecnológica del país.

La efectividad a largo plazo de estas disposiciones requiere fortalecer los sistemas de control; según datos de la SB (2023) revelan que apenas el 35% de las instituciones financieras cumple con auditorías externas anuales en materia de ciberseguridad, demostrando falencias en los procesos de supervisión. Si bien el artículo 50 de la LOPDP establece sanciones por incumplimientos, sería conveniente implementar exigencias adicionales como: La obtención de certificaciones internacionales como la ISO 27001 que acrediten sistemas robustos de gestión de riesgos y la publicación periódica de informes de transparencia de fácil acceso público. Este modelo, basado en el artículo 42 del RGPD, permitiría un seguimiento más sistemático además que convertiría la protección de datos en un factor de prestigio institucional, promoviendo una competencia por mejores prácticas (SB, 2023).

Adicionalmente, la eficacia de las políticas de salvaguarda de datos se basa esencialmente en la formación proactiva de los ciudadanos. Como evidencian Ordoñez y Valdivieso (2023), la educación digital potencia en 40% el efecto de estas regulaciones al capacitar a los usuarios para ejercer sus derechos. Si bien, la LOPDP en su artículo 8 reconoce oficialmente el derecho de acceso y rectificación, es indispensable la elaboración de estrategias pedagógicas más extensas. (LOPDP, 2021). Por lo tanto, vemos que la educación digital empodera al titular de los datos y reduce la asimetría informativa frente a las instituciones financieras, al punto de constituirse en la primera línea de defensa frente a los delitos informáticos en la banca electrónica. (Rivera y Maldonado, 2023)

Una propuesta concreta podría ser la puesta en marcha varias campañas con la colaboración con la Defensoría del Pueblo, las cuales estén orientadas principalmente a la instrucción de la población en lo referente a la presentación de denuncias por trasgresiones en sus datos personales y también en la configuración adecuada de las alternativas de privacidad en los programas financieros.

Además, se pueden proponer iniciativas como talleres comunitarios con guías interactivas cuyo fin seria reducir esta brecha que existe este momento en cuanto al reconocimiento legal de sus derechos. De esta manera los dueños de la información dejarían de ser sujetos pasivos para convertirse en actores activos conocedores de la importancia de su información personal.

Metodología

La investigación se realiza aplicando un enfoque cualitativo, el mismo que está centrado en realizar un análisis crítico tanto de los retos legales como operativos que supone la protección de la información personal específicamente en el sector financiero de Ecuador. Para ello se ha tomado principalmente un análisis documental que cubre tres aspectos fundamentales, por un lado, la valoración de los marcos regulatorios actuales, así como el análisis de casos judiciales destacados y la revisión de doctrina pertinente.

Esta metodología se encuentra elaborada con la investigación de varias fuentes, lo cual, facilita la valoración completa y efectiva de la aplicación de la LOPDP, es así que, el análisis cualitativo es especialmente apropiado para detectar diferencias entre el marco legal y su aplicación específica, y de la misma manera lograr sugerir mejoras en el sistema actual.

Se aborda derecho comparado para determinar y analizar las estipulaciones de la LOPDP y con este enfoque permitir en primera instancia, establecer un diálogo jurídico entre

el marco normativo ecuatoriano y estándares internacionales de referencia, particularmente el RGPD y, segundo lugar, buscar la implementación de una matriz de evaluación normativa especializada para facilitar el contraste sistemático entre la normativa y su aplicación concreta en las instituciones financieras, y de esta manera identificar tanto las brechas de cumplimiento existentes como los desafíos operativos que pueden enfrentar los organismos de control. SB (2023). Asimismo, el análisis incluye informes de organismos de control, tales como la Defensoría del Pueblo y la SPDP, para verificar la efectividad de las medidas adoptadas por las entidades financieras.

El universo de estudio está constituido por el sistema financiero ecuatoriano, dado su papel estratégico en la gestión de datos personales de millones de ciudadanos, además la investigación se apoya en la revisión de casos emblemáticos de vulneraciones de datos en instituciones bancarias y cooperativas, con el objetivo de evaluar el impacto de la normativa en la protección efectiva de los derechos de los titulares de datos (Mendoza, 2019).

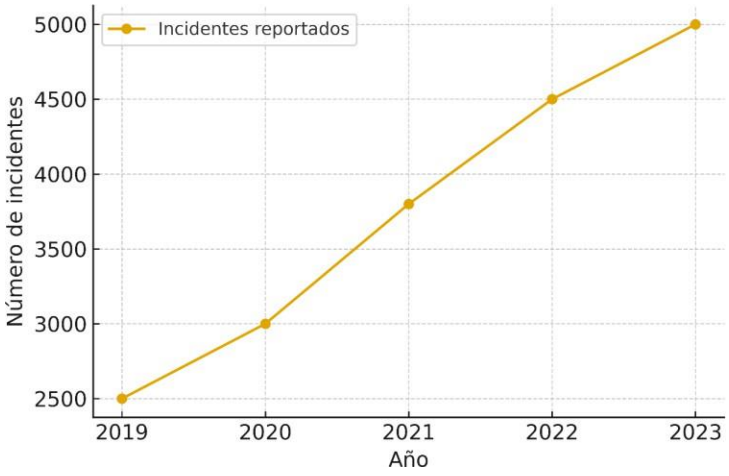
Finalmente, el tratamiento de la información recopilada se realizó mediante un análisis deductivo, contrastando la normativa nacional con su aplicación en la práctica, y mediante el método comparado, para evaluar la eficacia de las estrategias de protección de datos en el sector financiero en relación con estándares internacionales (Cevallos, 2023).

Resultados

La investigación evidenció un incremento del 30% en incidentes de seguridad en el sector financiero ecuatoriano desde 2019, superando los cinco mil casos en 2023.

Figura 1

Incremento de incidentes de seguridad en el sector financiero

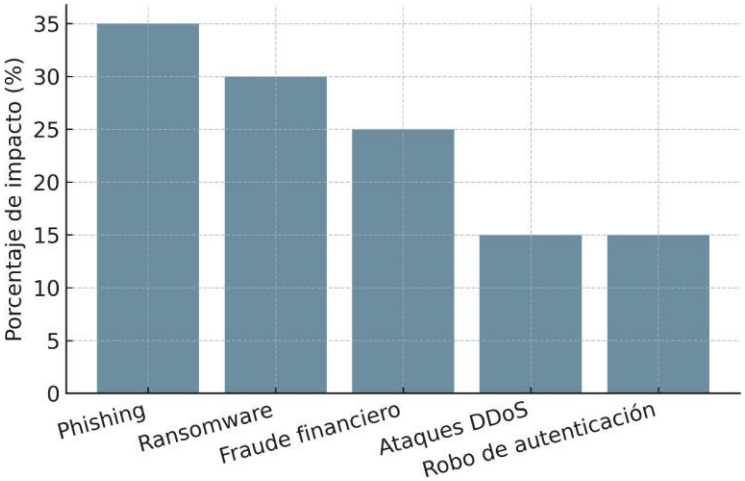


Fuente: datos de SB 2023 **Elaboración:** propia

Los ataques más frecuentes fueron phishing (35%), ransomware (25%), fraude financiero (20%), ataques DDoS (10%) y acceso no autorizado (10%).

Figura 2

Principales amenazas cibernéticas en la banca ecuatoriana



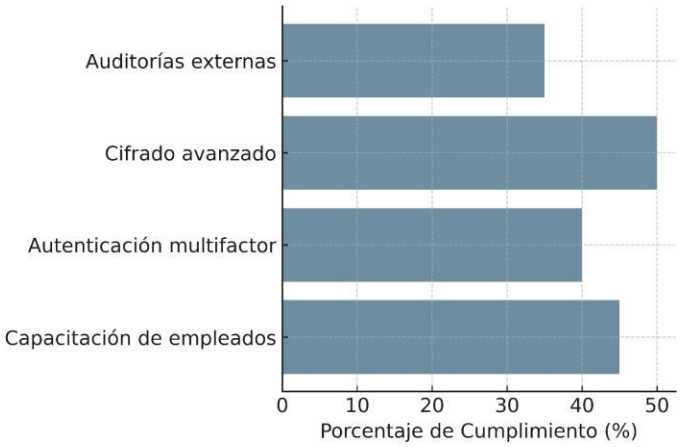
Fuente: datos de Guamán et al. 2023. **Elaboración:** propia

El nivel de cumplimiento de la LOPDP resultó deficiente: 35% de las instituciones realizaron auditorías de seguridad, 50% implementaron cifrado avanzado y 40% utilizaron

autenticación multifactorial.

Figura 3

Evaluación del cumplimiento de la LOPDP en el sector financiero

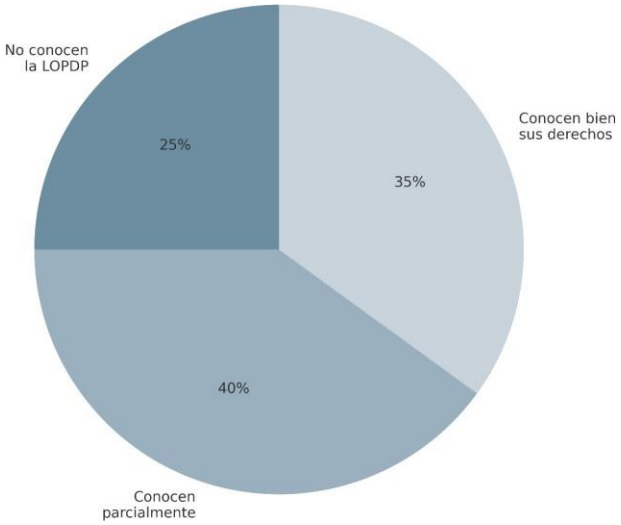


Fuente: datos de la SPDP, 2023. **Elaboración**: propia

El 35% de los clientes bancarios conoció sus derechos, mientras que un 25% desconoció la normativa.

Figura 4

Nivel de conocimiento de los clientes sobre la LOPDP



Fuente: datos de Defensoría del Pueblo, 2023. **Elaboración:** propia

Conclusiones.

En síntesis, los resultados y el análisis normativo permiten concluir que la mayoría de las entidades financieras ecuatorianas todavía no cumplen a cabalidad las evaluaciones de impacto ni las salvaguardias que exige la LOPDP, pues el contraste entre la normativa y la práctica resulta evidente, existen informes recientes de la SB que muestran que solo algo más de un tercio de las instituciones ha aplicado los análisis preventivos de riesgos que la ley considera indispensables, lo cual revela que la protección de los datos financieros, más allá de constituir un requisito administrativo, se ha convertido en un asunto de seguridad jurídica y de garantía efectiva de los derechos de intimidad y autodeterminación informativa reconocidos por la Constitución.

Frente a ese panorama, el artículo propone tres líneas de acción que se enraízan en la realidad institucional del país. Primero, una política de auditorías externas anuales registradas tanto en la SPDP como en la SB que permita verificar con independencia el estado real de las medidas de seguridad y, en su caso ordenar correcciones oportunas. Segundo, la creación de entornos controlados de prueba impulsados de manera conjunta por la banca privada y el Estado para ensayar tecnologías de detección temprana y respuesta a incidentes sin comprometer datos reales de los clientes y tercero un programa permanente de formación ciudadana, coordinado por la Defensoría del Pueblo, que capacite tanto a funcionarios como a usuarios sobre buenas prácticas digitales y sobre los mecanismos que ofrece la LOPDP para ejercer sus derechos.

La conjunción de fiscalización técnica, innovación regulada y educación social permitiría que la LOPDP deje de ser un marco declarativo y se convierta en un instrumento vivo de confianza pública, solo así el sistema financiero ecuatoriano podrá afrontar los riesgos de la

economía digital, preservar la competitividad internacional de sus servicios y, sobre todo, garantizar a la ciudadanía que su información personal permanece protegida en cada transacción.

Referencias

Asamblea Nacional. (2021, 26 de mayo). Ley Orgánica de Protección de Datos Personales. Registro Oficial No. 459.

Asamblea Nacional. (2014). Código Orgánico Monetario y Financiero. Registro Oficial Suplemento 332, 12 de septiembre de 2014.

Barrio Andrés, M. (2024). *Manual de derecho digital* (3ª ed.). Tirant lo Blanch.

Cámara de Fintech Ecuador. (2023). *Diagnóstico de capacidades tecnológicas en el sector financiero*. https://www.fintechecuador.org

Carvajal, A. (2022). Impacto del error humano en la filtración de datos en el sector bancario ecuatoriano. *Revista Latinoamericana de Seguridad Informática*, 10(2), 45-62.

Castro, M., Gómez, L., y Ramírez, J. (2023). Incentivos fiscales y cumplimiento de protección de datos: Lecciones desde Colombia. *Revista de Derecho Digital*, 8(2), 1-22. https://doi.org/10.5678/rdd.2023.0802

Cevallos Villa, J.A., y Lazo Martínez, J.M (2023). La protección de datos personales y el respeto a la privacidad en la legislación ecuatoriana. Universidad de Guayaquil, Facultad de Jurisprudencia, Ciencias Sociales y Políticas. https://repostitorio.ug.edu.ec/items/cf057aee- 9c83-4036-9acd-a475caaf240b

Comisión Económica para América Latina y el Caribe (CEPAL). (2021). *Informe sobre ciberseguridad en América Latina y el Caribe: Desafíos y oportunidades*. CEPAL. https://repositorio.cepal.org/

Defensoría del Pueblo del Ecuador. (2023). *Encuesta nacional sobre percepción de privacidad digital*. Recuperado de http://www.dpe.gob.ec

Diálogo Américas. (2022, abril 25). Ataques cibernéticos amenazan seguridad en Ecuador. Diálogo Américas. https://dialogo-americas.com/es/articles/ataques-ciberneticos-amenazan- seguridad-en-ecuador

González, M., y Andrade, R. (2020). Ciberseguridad en el sector financiero: Retos y soluciones desde América Latina. *Revista Iberoamericana de Derecho Digital*, 12(1), 78-95.

Guamán, M., Carrillo, J. A., Flores, C., y Ron, M. (2023). Análisis de riesgos y amenazas de ciberseguridad en el Estado ecuatoriano utilizando la metodología Magerit. *ProSciences: Revista de Producción, Ciencias e Investigación*, 7(2), 34-56.

Instituto Nacional de Ciberseguridad. (2019). Data leak from millions of Ecuadorians. INCIBE-CERT.https://www.incibe.es/en/incibe-cert/publications/cybersecurity- highlights/data-leak-millions-ecuadorians.

Journal of Economic and Social Science Research. (2024). El derecho a la protección de datos y el avance de las nuevas tecnologías en Ecuador: Implicaciones legales y éticas.

Lanas, G., y Cárdenas, G. (2023). La protección de datos personales en Ecuador: una revisión histórica-normativa. *ProSciences: Revista de Producción, Ciencias e Investigación*, 5(1), 57- 66.

Maldonado, L., y Vélez, A. (2022). *Cooperación público-privada en ciberseguridad: Experiencias desde Ecuador*. FLACSO Ecuador.

Mendoza Villegas, J. P. (2019). *La protección de datos personales en Ecuador: análisis comparativo con el Reglamento General de Protección de Datos (RGPD)*. Universidad Internacional de La Rioja (UNIR). https://ecuador.unir.net/actualidad-unir/expertos-

puntos- clave-ley-proteccion-datos-ecuador/

Ordóñez Pineda, L. O., y Valdivieso Ortega, G. J. (2023). El derecho a la educación digital: una oportunidad para afianzar un modelo de cultura digital para la paz. Revista de Cultura de Paz, 7, Art. 143. https://doi.org/10.58508/cultpaz.v7.143

Orellana Robalino, C. (2017). De la seguridad cibernética a la resiliencia cibernética aplicada a la protección de datos personales. *Foro Revista de Derecho, 27, 83-86.*

Paredes, J., y Salazar, K. (2021). Encriptación y protección de datos en la banca digital. *Revista de Ingenieríay Tecnología*, 15(2), 33-50. https://doi.org/10.33996/revistalex.v9i28.302

Rivera Pineda, Y. M., y Maldonado Ruiz, L. M. (2023). Vulneración del derecho a la privacidad dentro de la era digital en el Ecuador. *Pol. Con.*, (85), 982-1009. https://doi.org/10.23857/pc.v8i10.6172

Superintendencia de Bancos del Ecuador. (2023). *Informe sobre seguridad cibernética en el sector financiero ecuatoriano*. https://www.superbancos.gob.ec

Superintendencia de Bancos del Ecuador (2021). *Acciones de la Superintendencia frente al ciberataque a entidad controlada* https://www.superbancos.gob.ec/bancos/acciones-de-la-super-de-bancos-frente-a-ciberataque-de-entidad-controlada.

Superintendencia de Protección de Datos Personales. (2023). *Reporte de dependencia tecnológica en el sector bancario ecuatoriano*. https://www.gob.ec/spdp

Zuboff, S. (2021). *La era del capitalismo de vigilancia: La lucha por un futuro humano frente a las nuevas fronteras del poder*. Paidós.