593 Digital Publisher
CEIT
ISSN 2588-0705

Ley de Protección de Datos en Ecuador: implicaciones de riesgo existentes de ciberseguridad a los que puede estar expuesto el país de Ecuador con base en la ley de protección de datos

Data Protection Law in Ecuador: existing cybersecurity risk implications to which the country of Ecuador may be exposed based on the data protection law

Favio André Herrera-Llamba[1]
Pontificia Universidad Católica del Ecuador
faherral@pucesa.edu.ec

José Marcelo Balseca-Manzano[2]
Pontificia Universidad Católica del Ecuador
jbalseca@pucesa.edu.ec

doi.org/10.33386/593dp.2025.3.2668

V10-N3 (may-jun) 2025, pp 619-635 | Recibido: 20 de julio del 2024 - Aceptado: 10 de abril del 2025 (2 ronda rev.)

1 Estudiante de la maestría en Ciberseguridad - Pontificia Universidad Católica del Ecuador Sede Ambato
2 ORCID: https://orcid.org/0000-0003-1517-0013. Docente de la Pontificia Universidad Católica del Ecuador – Sede Ambtao, Escuela de Ingenierías. Magister en Gerencia Informática con mención en Desarrollo de Software y Redes.

Cómo citar este artículo en norma APA:

Herrera-Llamba, F., & Balseca-Manzano, J., (2025). Ley de Protección de Datos en Ecuador: implicaciones de riesgo existentes de ciberseguridad a los que puede estar expuesto el país de Ecuador con base en la ley de protección de datos. 593 Digital Publisher CEIT, 10(3), 619-635, https://doi.org/10.33386/593dp.2025.3.2668

Descargar para Mendeley y Zotero

RESUMEN

En la actualidad, la tecnología ha transformado profundamente la forma de vida y de trabajo, los datos que viajan por la red han dado lugar a una era digitalizada, sin embargo también se incrementa el robo de datos, violación de la privacidad y exposición de la información personal, la legislación ecuatoriana en cuanto se refiere a la Ley de Datos Personales es nueva, abarcando sanciones para la defensa nacional, el cuidado y buen almacenamiento de la información, No obstante, estas normativas aún se encuentran en una etapa inicial, especialmente si se comparan con las leyes de países europeos, en países de Latinoamérica toma una relevancia importante, el buen cuidado por parte del gobierno y su defensa nacional deben velar por sancionar a ciberdelincuentes y reducir las vulnerabilidades. Las empresas, ciudadanos y todos los que usan la red siempre dejan un rastro conocido como huella digital, que los expone a riesgos como adulteración o pérdida de datos, frecuentemente sin que los responsables sean identificados ni sancionados. En este contexto, se considera fundamental realizar una revisión sistemática de la legislación en materia de protección de datos en los diferentes países de Latinoamérica. Este análisis comparativo y descriptivo permitirá identificar las similitudes, diferencias y puntos críticos de estas normativas, además de determinar qué información se considera más sensible en términos de protección. la metodología utilizará principalmente la revisión bibliográfica de documentación de fuentes primarias, secundarias, tesis y artículos científicos. Destacando la importancia de reducir las brechas de seguridad y de sancionar de manera efectiva.

Palabras claves: privacidad; ciberdelincuentes; legislación; protección de datos; vulnerabilidades.

ABSTRACT

Currently, technology has profoundly transformed the way of life and work, the data that travels through the network has given rise to a digitalized era, however, data theft, violation of privacy and exposure of information are also increasing. personal information, Ecuadorian legislation regarding the Personal Data Law is new, covering sanctions for national defense, care and good storage of information. However, these regulations are still in an initial stage, especially if are compared with the laws of countries Europeans, in Latin American countries it takes on important relevance, good care on the part of the government and its national defense must ensure that cybercriminals are punished and vulnerabilities are reduced. Companies, citizens and everyone who uses the network always leave a trace known as a digital footprint, which exposes them to risks such as adulteration or loss of data, often without those responsible being identified or punished. In this context, it is considered essential to carry out a systematic review of data protection legislation in the different Latin American countries. This comparative and descriptive analysis will make it possible to identify the similarities, differences and critical points of these regulations, in addition to determining what information is considered most sensitive in terms of protection. The methodology will mainly use the bibliographic review of documentation from primary sources, secondary theses and scientific articles. Highlighting the importance of reducing security breaches and sanctioning effectively.

Keywords: privacy; cyber criminals; legislation; data protection; vulnerabilities.

Introducción

A nivel mundial todos los días viajan datos personales de millones de personas por la red, el alcance del internet se ha disparado gracias al confinamiento de COVID que freno todo trabajo de forma presencial y lo traslado a los hogares, basta tener conexión a la red para tener acceso todas las plataformas, sitios web y redes sociales, es normal compartir los datos de DNI, nombres, correo y un teléfono celular, en sitios financieros, académicos, laborales, de la salud, comunicación, comercios electrónicos entre otros, el problema se da porque no se mide las consecuencias de qué forma serán tratados estos datos, con su contrapartida de fraudes desde virus, pishing, llamadas telefónicas falsas, robo de identidad.

La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. (Diario Oficial UE, 2016)

Tener una conexión de internet estable y continua se puede considerar ahora como algo de vida o muerte. La educación, la salud, el trabajo, todos estos sectores dependen de un buen acceso a medios digitales que nos permitan estar conectados y sobrellevar la pandemia. En América Latina, la región del mundo más golpeada por la covid-19, el acceso digital dista de ser idóneo: menos de la mitad de los latinoamericanos tienen conectividad de banda ancha fija y solo el 10% cuenta con fibra de alta calidad en el hogar. (Banco Mundial, 2021)La pandemia ocasiono cambios importantes en el uso de tecnologías digitales alrededor del mundo. A efectos de analizar cómo ha evolucionado el nivel de digitalización de cada país durante el año 2020, en primer lugar, se analiza el nivel de adopción de servicios fijos y móviles. (Jung & Katz, 2023)

Todas las normativas de Ley de Protección de Datos parten desde las leyes europeas, con sanciones muy severas que pueden ser desde los 20 millones de euros o el 4 % de su volumen anual en el negocio. Modernizándose en 1995, adoptado en 2016 y en vigencia a nivel europeo desde 2016. Con un Comité Europeo de Protección de Datos con 27 representantes de control independiente.

A nivel de Ecuador se dieron varias fallas de vulneración a sistemas desde la caída de una de los bancos más grandes del país, otras afectaciones como se dio a la empresa pública de telecomunicaciones y en servicios en municipios, aunque fueron noticias muy sonadas de forma interna en el país, pero al no tener una Ley de Protección de Datos las instituciones mismo resolvieron los inconvenientes donde la perdida no solo fue económica sino también de información de socios, clientes. En las últimas horas, hemos identificado un incidente de ciberseguridad en nuestros sistemas informáticos que han deshabilitado parcialmente nuestros servicios. Hemos tomado medidas inmediatas como aislar los sistemas potencialmente afectados del resto de nuestra red y tenemos expertos en ciberseguridad para ayudar en la investigación. (Banco Pichincha, 2021). En el mes de julio, CNT (Corporación Nacional de Telecomunicación) fue víctima de un ataque informático, del que aún no se conocen las intenciones. Esto pone en el objetivo las políticas de ciberseguridad con el que deben contar todas las empresas e instituciones y que da de qué hablar en el Ecuador.(CNT, 2021). Franz Enríquez, director de Tecnologías e Informática del Municipio de Quito, señaló que el ataque informático tenía como objetivo dejar indisponible toda la información e infraestructura tecnológica. El 15 % de la información de la base de datos de la administración central del cabildo fue afectado, hasta que se logró contener el virus, acotó.(MDMQ, 2022)

Método

Realizar una revisión sistemática de Literatura de las diferentes leyes entre los países de Latinoamérica para validar que información es la más sensible dentro de ley de protección de datos, Para ello, se utilizará un enfoque comparativo

y descriptivo, revisando las similitudes y diferencias entre leyes que han surgido en Latinoamérica. la metodología utilizará principalmente es la revisión bibliográfica de documentación de fuentes primarias como; boletines gubernamentales, memorándums, registros oficiales, investigaciones secundarias; tesis, artículos científicos, periódicos, boletines de prensa. Con un enfoque cuantitativo de los problemas más comunes que sufren las empresas al no cuidar de forma adecuada sus datos y las posibles sanciones que están expuestas a nivel Latinoamericano, tomando como base los datos secuestrados diariamente en el Ecuador, mostrando la perdida de datos a causa de no haber implementado leyes cuando ocurrieron las primeras vulnerabilidades en el país.

La recopilación e investigación brinda un enfoque de confiabilidad para obtener data confiable de artículos científicos, políticas, legislaciones de otros países como referentes para un investigación adecuada con documentos que aporten a la investigación, se valida información de empresas que brindan servicio de protección de antivirus y presentan informes de vulnerabilidades frecuentes, toda la investigación obtenida permitirá enfocarse en tener criterios para poder construir un (SGSI) Sistema de Gestión de Seguridad de la Información para mitigar vulnerabilidades y cumplir el reglamento establecido en el marco legal ecuatoriano, el riesgo cero no existen pero con implementar políticas se minimiza la amenazas que diariamente están apareciendo.

Investigación

La ausencia de una ley de protección de datos personales en Ecuador represento un riesgo significativo para la seguridad y privacidad de las personas. En un mundo donde la información personal se ha convertido en un recurso valioso, la falta de regulación adecuada deja a los ciudadanos vulnerables a amenazas como el robo de identidad, la filtración de información confidencial y el indebido uso de los datos, al ocurrir ya la fuga de data en Ecuador graves errores como no haber implementado leyes de forma inmediata que regularice y sancionen culpables, permitió que sigan existiendo incidencias, en los diferentes gobiernos precursores, los ecuatorianos han estado expuestos a la perdida de información tomando ejemplos y casos muy sonados como en el año 2018 con los problemas ocurridos en la empresas públicas CNT y la alcaldía de Quito, sufrieron robos de información por parte de ciberdelincuentes, el banco más grande del Ecuador Banco Pichincha estuvo por dos meses casi con problemas de operación, estás noticias a nivel interno no sonaron tan fuerte a diferencia del nivel internacional donde exigían que el gobierno debe hacer algo al respecto para mitigar este tipo de vulnerabilidades que también perjudica los datos personales.

Los riesgos que conlleva no proteger los datos son de gran impacto, los datos personales mal custodiados o perdidos al ser ya comprometidos pueden ser utilizados para suplantar la identidad de las personas, los delincuentes pueden abrir cuentas bancarias, solicitar créditos o realizar compras en su nombre. Al tener la información como números de tarjetas de crédito, puede ser utilizada para realizar transacciones fraudulentas, la exposición de datos personales, como direcciones de empleo o trabajo, números de teléfono y correos electrónicos, puede resultar en un incremento de spam, acoso y violaciones de la privacidad, al ser víctima de un hackeo o pérdida de datos y no poder acceder a las cunetas esto también puede causar ansiedad y preocupaciones sobre la seguridad personal y financiera, las cuentas y redes sociales comprometidas pueden ser utilizadas para realizar ataques a otras personas, chantajes, insultos o daños a sistemas donde se tenga privilegios de alta gerencia o ser personal ejecutivo, a menudo sin el conocimiento del propietario de la cuenta o empresa.

La suplantación de identidad, el hackeo y robo de toda información, las llamadas de empresas sin consentimiento, entre otras formas de que vulneren los datos personales son noticias diarias, con el alcance del internet y la llegada a lugares lejanos la gente se entera de que sus datos están siendo utilizados de una mala manera, desde exposición de bancos en el año 2021 como lo ocurrido en el banco de austro con la explosión de datos de clientes, Pronaca en el 2022 la filtración

de datos de empleados, en el 2022 la noticia más polémica y que estuvo expuesta a nivel mundial con la brecha de seguridad a las bases de datos de los usuarios de Banco Pichincha, exposición de datos de pasajeros en vuelos en el 2023 y robo de datos no consentidos de entidades públicas como municipios.

En 2023 entra en Vigencia en Ecuador la Ley de protección de datos personales, en el 2024 es elegido el Super intendente de Protección de datos personales. Para que las empresas traten de mejor manera los datos personales, que exista sanción en contra de los que vulneren la información, pero para la construcción de toda esta Ley se realizaron debates en la Asamblea Nacional, se trajo expertos de diferentes países de Latinoamérica y Europa, para que con su experiencia la Ley sea aplicada acorde a la constitución del país. Se quiere evitar también que la huella digital que se deja en la red, no atente contra la información del usuario para campañas publicitarias u ofertas mediante llamadas telefónicas, salvaguardar la información de personal con enfermedades graves o resguardar historias clínicas. pero la desinformación o al no tener claras las políticas que defienden al consumidor no se las aprecia de forma Clara, dando paso a que los datos no sean tratados de la forma adecuada, el almacenamiento no esté bien protegido.

Tabla 1
Secuestros de Datos diarios Ecuador

Secuestro de Datos	
Secuestros	500
Vulnerabilidades	350
Correos Maliciosos	150k
País	Republica de Ecuador
Clasificación Global	58
Número de Usuarios	0,16%

Fuente NGS SecurityLogic - (Balseca, 2024)

En el evento presentado en el mes de Junio por SecurityLogic, con el tema de las 7 capas de Ciberseguridad en el Sector Financiero, nos muestra cifras del Ecuador donde de todo los países atacados a nivel mundial estamos en el puesto número 58 de ranking y propensos a vulnerabilidades que afectan la información de los usuarios, 150.000 correos maliciosos están llegando a bandejas de entradas con la intención de robar información mediante ataques de pishing, páginas falsas, links con código malicioso, archivos ejecutables, los cibercriminales secuestran datos de al menos 500 personas y tratan de obtener un rescate que sea tipo financiero, las vulnerabilidades que buscan explorar son aproximadamente de 350 registros que nos presenta. Con la pandemia y el cambio tecnológico, comercios electrónicos, pagos de productos con transferencias o tarjetas bancarias, también traslado a que al menos los ciudadanos tengan una cuenta bancaria, el enfoque de ataque del mundo físico se trasladó a la digital para obtener beneficios económicos de empresas o personas que no cuidan sus datos en la red o acumulan grandes cantidades de dinero sin mirar a los peligros que está expuestos en la red.

Se habla de muchos convenios que el Ecuador ha realizado en materia de Ley de Protección de Datos, con el dictamen por parte de la Corte Constitucional en Ecuador en marzo 2024, Fabián Iñiguez menciona que El Convenio de Budapest, también conocido como el Convenio sobre Ciberdelincuencia, es un tratado internacional diseñado para ayudar a proteger a las sociedades contra los delitos informáticos y su objetivo principal es armonizar las leyes nacionales relacionadas con la ciberdelincuencia, mejorar las capacidades de investigación de los delitos tecnológicos a nivel internacional y aumentar la cooperación entre las naciones para enfrentar eficazmente las amenazas de ciberdelitos. (Iñiquez, 2024)

Tabla 2
Casos de vulneración de datos a empresas ecuatorianas

Empresa	Fecha del Ataque	Tipo de Ataque	Acciones Tomadas	Artículo de la Ley de Protección Vulnerado	**Fuentes**
Corporación Nacional de Telecomunicaciones (CNT)	jul-2021	Fuga de datos	Notificación a los usuarios afectados, investigación del incidente, implementación de medidas de seguridad adicionales.	Art. 9: Seguridad de los datos personales	(CNT, 2021)
Servicio de Rentas Internas (SRI)	Jul-2021	Ataque DDoS	Implementación de medidas de mitigación DDoS, investigación del incidente, fortalecimiento de la infraestructura tecnológica.	Art. 10: Confidencialidad de los datos personales	(SRI, 2021)
Banco Pichincha	oct-2021	Ransomware	Restauración de sistemas a partir de copias de seguridad, pago de rescate (no confirmado), implementación de medidas de seguridad adicionales.	Art. 11: Protección de datos personales	(SB, 2021)
Agencia Nacional de Tránsito (ANT)	Oct-21	Malware	Suspensión de servicios en línea, investigación del incidente, implementación de medidas de seguridad adicionales.	Art. 12: Tratamiento de los datos personales	(ANT, 2021)
Municipio de Quito	Abril-2022	Ransomware	Restauración parcial de sistemas a partir de copias de seguridad, negociación con los actores de la amenaza, implementación de nuevas medidas de seguridad.	Art. 13: Acceso a los datos personales	(Ochoa, 2022)

Los casos de vulneración a empresas ecuatorianas muestran que empresas desde el sector financiero hasta empresas públicas son afectadas por ciberdelincuentes que encuentran brechas de seguridad en los sistemas y de alguna manera buscan tener una compensación de forma económica, la mayor parte de estos ataques parten desde una previa recolección de datos y el ataque que realizan es planificado, las afectaciones a los datos van desde robo de información personal hasta robo de cuentas bancarias, robo de identidad y todo esto es ya considerado delitos en contra de La Ley de Protección de datos que entra en vigencia desde el 2023. La Secretaria de Protección de Datos Personales es la entidad encargada de velar por el cumplimiento de la Ley Orgánica de Protección de Datos Personales y garantiza que las empresas que no cumplan con esta ley son objeto de sanciones administrativas, como multas, la suspensión de actividades y son obligadas de reparar el daño causado.

Tabla 3

Algunas leyes, normativa y convenios desarrollados desde el estado a favor de la seguridad de la información y ciberseguridad.

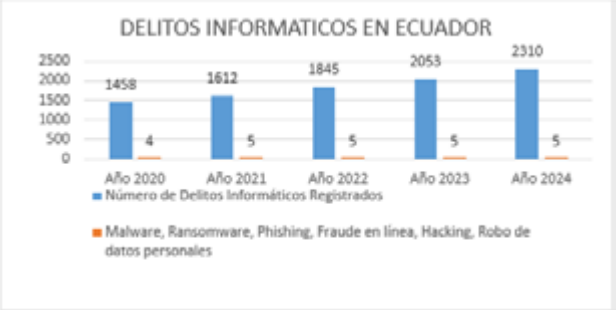
Norma/proyecto, ley, convenio	Fecha de publicación	Fuente
Superintendencia de Bancos: Norma de control para la gestión del riesgo operativo	01/12/2021	(SuperintendenciaDe-Bancos, 2021)
Convenio sobre ciber-delincuencia (Convenio de BUDAPEST)	Marzo del 2022, Ecuador está en calidad de «observa-do».	(COE, 2022)
Superintendencia de Economía Popular y Solidaria. Norma de Control respecto a la Seguridad de la Infor-mación	01/05/2022	(SEPS, 2022)
Estrategia Nacional de Ciberseguridad del Ecuador	01/08/2022	(MINTEL, 2022)
Ley Orgánica para la Transformación Digital y Audiovisual	01/02/2023	(GobiernoElectronico 2023)
Reformas al COIP – Ley orgánica reformatoria a varios cuerpos legales para el fortalecimiento de las capacidades institucio-nales y la seguridad integral	01/03/2023	(RegistroOficial, 2023)
Esquema Gubernamen-tal de Seguridad de la Información EGSI V3	1/3/2024 El EGSI es de imple-mentación obligatoria en las entidades, organismos e instituciones del sector público	(MINTEL, 2024)
Ley Orgánica de Seguri-dad Digital	Para segundo debate en la Asamblea Nacional del Ecuador posiblemente se publique en este primer semestre del 2024	(AsambleaNacion-al,2023)

Fuente ITAhora, (Iñiquez, 2024)

Desde los hechos ocurridos en pandemia de ataques a diferentes instituciones, robo de información la presión ejercida por otros países a Ecuador toma más en serio mejorar las leyes para mitigar los riesgos que se puedan presentar en el país en materia de seguridad de la información, partiendo desde el 2021 con normas de control en la parte de riesgos para los bancos, participación en el convenio de BUDAPEST como observador en el año 2022, la SEPS con su normativa de control para seguridad de la información en 2022 y este mismo año en el mes de agosto dar un paso extra con la Estrategia Nacional de Ciberseguridad del Ecuador, 2023 un año para cambios en la Ley Orgánica para la Transformación digital, reformas en el COIP sobre la seguridad integral en instituciones, la versión 3 de implementación obligatoria de entidades del sector público del Esquema Gubernamental de Seguridad de la Información. En este año 2024 se espera la publicación de la Ley Orgánica de Seguridad Digital.

Figura 1

Delitos informáticos en Ecuador



Fuentes: Ministerio del gobierno, Policía Nacional y Arcotel, (MisiteriodeGobierno, s. f.) y (FGE, s. f.)

Al filtrar varias fuentes de información de la Fiscalía General del Estado, los periódicos Primicias y El comercio, la figura muestra el aumento de delitos informáticos que se llevan a cabo en Ecuador, hasta el 2020 el malware era una de los principales delitos que se denunciaban, pero desaparecen en los siguientes 4 años posteriores, desde el 2021 se suma a la lista de los mayores delitos registrados el rasomware, los delitos que se mantienen durante todos los años son; pishing, fraudes en líneas, hacking y el robo de datos. En comparación al año 2020 donde se presentan 1458 delitos informáticos el año 2024 presenta 2310 ataques una diferencia de 852 lo cual denota que en 4 años existen más de 200 delitos más cometidos que van en tendencia de subida.

Según Luis Enríquez "¡El Reglamento General de Protección de datos (RGPD) cambió al mundo! es un decir popular en la actualidad. La verdad es que el RGPD responde a una larga evolución sobre la protección de datos personales en la Unión Europea de más de 40 años, que ha influenciado en otras regiones del mundo, entre ellas Latinoamérica. La aplicación directa del RGPD y su alcance extraterritorial hacen que instituciones públicas y privadas de todo el mundo deban cumplir con las obligaciones en él establecidas, incluidas las latinoamericanas." (Enríquez, 2021), tener referencias de países donde la ley está vigente, ayuda a los demás países a la propia construcción se políticas nacionales el trabajo conjunto entre naciones para evita incidencias con la información, de la misma forma aumenta en una región el cumplimiento de las normativas.

El Convenio número 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo; el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico, y el Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, entre otros.(RIPD, 2016). La protección de los datos personales y el respeto de la vida privada son derechos fundamentales europeos. El Parlamento Europeo ha insistido siempre en la necesidad de lograr un equilibrio entre el refuerzo de la seguridad y la tutela de los derechos humanos, incluida la protección de los datos y de la vida privada. Las nuevas normas de la Unión en materia de protección de datos, que refuerzan los derechos de los ciudadanos y simplifican las normas para las empresas en la era digital, entraron en vigor en mayo de 2018.(Marti y Maciejewski, 2024). La 30ª Conferencia Internacional de Autoridades Protección de Datos y Privacidad adoptó en Estrasburgo unánimemente la Resolución relativa a la urgente necesidad de proteger la privacidad en un mundo sin fronteras, y de alcanzar una propuesta con junta para el establecimiento de estándares internacionales sobre privacidad y protección de datos personales.(Novoa, 2020)

Téngase en cuenta que el uso de las nuevas tecnologías ha añadido una dosis importante de comodidad y celeridad tanto en el procesamiento de los datos como en su intercambio, lo cual genera un importante trasiego de información a nivel mundial. Y es justo ese contexto el que genera una indefensión de las personas en relación a la protección de sus datos personales en todas las partes del mundo, ya sea que se disponga de legislación local en materia de protección de datos o no. (Santamaría, 2020). El país más afectado de la región es Brasil con 603 mil intentos de ataque durante el periodo observado (ocupando el 4º lugar en la lista global). Le siguen Ecuador con 212,000 (de los cuales 139,000 fueron realizadas por WannaCry), México (102,000 – 8,000 de los cuales fueron por el grupo Encoder), Colombia (80,000, 48,000 de estas del grupo Hive), Chile (46,000 (de los cuales 500 ataques fueron realizados por LockBit) y Perú (31,000, de los cuales 2,5 mil fueron realizados por Stop). (Kasperky, 2023)

El estudio también revela que la falta de conciencia sobre la legislación de protección de datos afecta a las empresas en la región. Un preocupante 47% de ellas no capacita a sus empleados sobre la normativa vigente. Empresas chilenas y argentinas lideran este descuido con un 57% y un 56%, respectivamente. De manera sorprendente, solo el 32% de los usuarios encuestados afirmó recibir capacitación en sus empresas sobre protección de datos. Expertos advierten que la negligencia de los empleados es la principal puerta de entrada para los ciberdelincuentes, lo que puede resultar en filtraciones de información confidencial y multas severas para las empresas. (PrensarioTI, 2024)

Ante este panorama, la colaboración internacional se hace obligatoria, tanto por el tema jurisdiccional, como por el aspecto normativo y de seguridad. Ello resulta funda mental para poder generar confianza y tranquilidad en las personas, en el sentido de que los países están trabajando en proteger la intimidad de los datos personales de sus connacionales, y que no se haga un uso indebido de la información personal que pueda

generar daños irreparables.(Robles Osollo, 2021)urge the legal systems for and adequate protection, the information exchange between countries, such as health, politics, trade and the use of new technologies, as well as the possible collision with the right of access to information. The analysis of the European regulations to protect data, as well as the reception of Mexican regulations as a leading Latin American country and a signatory of the Convention 108 of Strasbourg is paramount.",",container-title":"Revista Eurolatinoamericana de Derecho Administrativo","DOI":"10.14409/redoeda.v8i1.9543","ISSN":"2362-583X","issue":"1","journalAbbreviation":"Rev. Eurolatin. Derecho Adm.","language":"es","license":"http://creativecommons.org/licenses/by/4.0","page":"35-60","source":"DOI.org (Crossref. Contar con unas buenas medidas de seguridad en nuestra red es uno de los aspectos principales, los hackeos informáticos se basan en ello. Es alguna los virus informáticos, los robos de identidad intrusiones pertenecen a los delitos que se dan en la red y estos fallos pueden provocar daños muy graves y en la mayoría de los casos irreparables. (Robles Osollo, 2021)urge the legal systems for and adequate protection, the information exchange between countries, such as health, politics, trade and the use of new technologies, as well as the possible collision with the right of access to information. The analysis of the European regulations to protect data, as well as the reception of Mexican regulations as a leading Latin American country and a signatory of the Convention 108 of Strasbourg is paramount.",",container-title":"Revista Eurolatinoamericana de Derecho Administrativo","DOI":"10.14409/redoeda.v8i1.9543","ISSN":"2362-583X","issue":"1","journalAbbreviation":"Rev. Eurolatin. Derecho Adm.","language":"es","license":"http://creativecommons.org/licenses/by/4.0","page":"35-60","source":"DOI.org (Crossref Las naciones pueden tener las mejores protecciones en sus sistemas, pero para desestabilizar un gobierno siempre habrá hacker que con su poder quieren hacer daño a la nación no les importa los datos que roben sino el resultado de dejar su huella y en este caso robar dinero para que las naciones vean su poder y que no están protegidas al 100%.

En la actualidad el mundo atraviesa una revolución digital en el cual la IA tiene un papel importante para su desarrollo. Una óptima implementación, garantiza un resultado positivo para el análisis de la información. Al ser una herramienta que permite tener acceso y recolección de datos personales, se debe asegurar de tener estándares rigurosos para el uso adecuado y su protección aún más relacionadas a entidades financieras. (Barrero, Vergara, y Chaves, 2023) La inteligencia Artificial puede mejorar los sistemas de seguridad en la recolección de datos al revisar si la documentación entrante tiene demasiada información y si esta es muy sensible, catalogándola y etiquetándola según los criterios de sensibilidad. Software a disposición existe, construcción de aplicaciones para analizar documentación existe, pero por la gran cantidad de información que puede tener una empresa también los costes son elevados.

Tabla 4

Vulnerabilidades en Latinoamérica y relación con la ley de Protección de datos de Ecuador

Empresa	País	**Fecha**	**Tipo de ataque**	**Acciones tomadas**	**Ley vulnerada (país)**	**Artículo similar (Ley de Protección de Datos de Ecuador)**	**Posibles sanciones (país)**	**Fuente del ataque suscitado**
Grupo Bancolombia	Colombia	sep-21	Ransomware	Restauración de sistemas a partir de copias de seguridad, pago de rescate (no confirmado).	Ley 1237 de 2009	Art. 16: Protección de datos personales	Multas hasta 1.700 salarios mínimos mensuales legales vigentes, cierre temporal o definitivo del establecimiento.	(González, 2024)
Travelex	Latinoamérica	ene-20	Ransomware	Suspensión de operaciones, restauración de sistemas a partir de copias de seguridad, pago de rescate.	Ley 10.973/2003 (Brasil)	Art. 7: Principios básicos para el tratamiento de datos	Multas de hasta R$ 50 millones, cierre temporal o definitivo de la empresa.	(CERT.ar, 2022)
EPM (Empresas Públicas de Medellín)	Colombia	dic-22	Ransomware	Restauración de sistemas a partir de copias de seguridad, no se pagó rescate.	Ley 1237 de 2009	Art. 16: Protección de datos personales	Multas hasta 1.700 salarios mínimos mensuales legales vigentes, cierre temporal o definitivo del establecimiento.	(MINTIC, 2022)
Latam Airlines	Chile	mar-21	Violación de datos	Notificación a los clientes afectados, implementación de medidas de seguridad adicionales.	Ley 19.628 (Chile)	Art. 4: Principios para el tratamiento de datos personales	Multas de hasta 10.000 Unidades de Fomento, cierre temporal o definitivo de la empresa.	(ANCI, 2021)
Kaseya	Latinoamérica	jul-21	Ransomware	Restauración de sistemas a partir de copias de seguridad, pago de rescate por parte de algunos clientes.	Ley de Protección de Datos Personales de cada país	Art. 16: Protección de datos personales	Multas de acuerdo a la Ley de Protección de Datos Personales de cada país, cierre temporal o definitivo de la empresa.	(KASEYA, 2021)
Comisión Nacional de Valores (CNV)	Argentina	oct-23	Ransomware	Suspensión de actividades, restauración de sistemas a partir de copias de seguridad.	Ley 25.326 (Argentina)	Art. 16: Protección de datos personales	Multas de hasta 3.000.000 de pesos argentinos, inhabilitación para realizar actividades en el mercado de valores.	(Argentina.gob.ar, 2023)
Garbarino	Argentina	ago-23	Ransomware	Suspensión de ventas online, restauración de sistemas a partir de copias de seguridad.	Ley 25.326 (Argentina)	Art. 16: Protección de datos personales	Multas de hasta 3.000.000 de pesos argentinos, inhabilitación para realizar actividades en el mercado de valores.	(Lezama et al., 2023)
GTD	Chile y Perú	oct-23	Ransomware	Afectación de servicios de data center, telefonía, VPN e internet. Restauración de sistemas a partir de copias de seguridad.	Ley 19.628 (Chile) y Ley 29733 (Perú)	Art. 4 (Chile) y Art. 15 (Perú): Principios para el tratamiento de datos personales	Multas de hasta 10.000 Unidades de Fomento (Chile) y –hasta 400 UIT (Perú), cierre temporal o definitivo de la empresa	(CSIRT.TELCONET, 2023)

593 Digital Publisher CEIT ISSN 2588-0705

Países de Latinoamérica han sido atacados con uno de los virus más famosos en estos últimos años que es Ransonware, un tipo de virus que cifra los archivos de los equipos infectados y depende el ciberdelincuente este puede pedir una compensación económica super fuerte por medio de Bitcoins un tipo de moneda digital, para no ser rastreado dentro de la red, este virus puede afectar toda una empresa, dependiendo el daño que se quiera hacer, la detención de las operaciones, bloqueo e ingresos al sistemas web, vulneración y robo de los datos personales de los clientes de esa empresa, mala reputación por no brindar las garantías al usuario, problemas con las autoridades de cada país, al mismo tiempo si una empresa tiene copias de seguridad y tienen estructurado un buen SGSI puede dar de baja el sistema contaminado y restaurar una copia reciente, pérdidas económicas existirán pero el negocio continuara.

Tabla 5

Delitos más comunes en Latinoamérica, leyes semejantes y sanciones

Tipo de Ataque/ sanciones	**Robo de Datos Personales**	**Malware**	**Ataque de denegación de Servicios DoS**	**Prisión**	**Sanciones**	**Fuente**
Descripción/País	Obtención no autorizada de datos personales, como nombres, direcciones, números de teléfono o información financiera.	Software malicioso que se instala en un dispositivo sin el consentimiento del usuario, con el objetivo de causar daño o robar información.	Inundación de un sistema con tráfico falso para hacerlo inaccesible para los usuarios legítimos.			
Ley de Protección de datos Ecuador	Art. 16: Protección de datos personales	Art. 18: Seguridad de los datos personales	Art. 20: Seguridad de la red y de los sistemas de información	hasta 1 año de prisión	Multas de hasta 37.000 dólares estadounidenses (Ecuador)	(Lexis, 2021)
Ley de Protección de datos Colombia	Art. 16 (Protección de datos personales	Art. 17 (Seguridad de los datos personales)	Art. 19 (Seguridad de la red y de los sistemas de información)	hasta 5 años de prisión	Multas de hasta 1.700 salarios mínimos mensuales legales vigentes	(FuncionPublica, 2012)
Ley de Protección de datos Brasil	Art. 7 (Principios básicos para el tratamiento de datos)	Art. 8 (Deberes del responsable del tratamiento)	Art. 9 (Seguridad de la información)	hasta 2 años de prisión	Multas de hasta R$ 50 millones	(Planalto, 2018)
Ley de Protección de datos Chile	Art. 4 (Principios para el tratamiento de datos personales	Art. 10 (Seguridad de los datos personales)	Art. 11 (Seguridad de la red y de los sistemas de información)	hasta 3 años de prisión	Multas de hasta 10.000 Unidades de Fomento	(LeyChile, 2023)
Ley de Protección de datos Perú	Art. 15 (Principio de seguridad de los datos personales)	Art. 19 (Deberes del responsable del tratamiento)	Art. 20 (Seguridad de la red y de los sistemas de información)	hasta 4 años de prisión	Multas de hasta 400 UIT	(ElPeruano, 2011)
Ley de Protección de datos México	Art. 26 (Protección de datos personales)	Art. 28 (Seguridad de los datos personales)	Art. 30	hasta 6 años de prisión	Multas de hasta 800,000 pesos mexicanos	(CongresodelaUnion, 2017)

Los ataque más comunes a nivel de Latinoamérica siguen siendo el robo de datos personales, estos pueden deberse a la Fuga de Información de empresas, la huella digital dejada en sititos web y el famoso Pishing, El software malicioso que se puede ejecutar en computadores puede suceder por instalar programas con activadores infectados de virus, dispositivos de almacenamiento masivo con virus, archivos descargables y links con acceso a paginas no seguras, el ataque de DoS o denegación de servicios es un ataque de envió de muchas peticiones para sobrecargar un servidor y este colapse al no poder responder a todos los servicios que están consultando y este tráfico se colapsa. Al mirar las leyes de otros países con las leyes de Ecuador, están enfrascado en la protección de datos personales, los principios de seguridad con los datos, la seguridad en la red, la seguridad de los sistemas información y se indaga más a profundidad siempre existe un responsable que debe estar al pendiente, cuidado, almacenamiento y el correcto tratamiento que se le a los datos, las sanciones que se aplican en este caso van desde el un año de prisión dependiendo el país hasta más de los 6 años esto también depende de la madurez de la Ley, ya que mientras más reformas o cambios realizados las sanciones aplicadas son más drásticas a diferencia de Ecuador como en una nueva ley está se debe ir mejorando.

Discusión

Dentro de ciberespacio encontramos gran cantidad de información muchas de las veces entes gubernamentales comunican a la ciudadanía que la información de ellos es publica y que cualquier persona en el mundo puede revisar, los datos primarios no deberían estar expuestos, se debería enmascarar o el titular debería presentar una identificación para poder obtener esta información, las leyes a aplicarse deben ser entre pilares fundamentales la ciberseguridad, la seguridad informática y seguridad de la información, términos que se creen son iguales, no los son pero la relación entre ellos para la protección se basa en la protección de la data en sus diferentes niveles, pero la que más abarca en este mundo tecnológico y mayor énfasis en el cuidado de la red es la ciberseguridad, es bueno que se vaya de a poco integrando estos términos a la ciudadanía en conjunto con los avances tecnológicos,, una visión mayor de donde debe estar enmarcado la ley, con sus diferentes reformas no tenerle miedo a la resiliencia cibernética, al materializarse un delito los ciberdelincuentes toman a su favor las leyes que les permiten infringir por mayor tiempo una vulnerabilidad encontrada hasta que estado subsane este hecho.

El aporte que la Ley de Protección de Datos de Ecuador, marca un precedente en mejorar la seguridad de todos los ciudadanos, después de haber perdido información en entidades bancarias y grandes bases de datos en el sector público. que Lo cual conlleva a que debe sea más relevante el tema. Tratar de mejor manera los datos personales permite entre países un mejor control en mantener protegidos a los ciudadanos. A los ecuatorianos darles a conocer la estrategia nacional de ciberseguridad difundida el 5 de agosto de 2022 para tomar en cuenta los 6 planes que lo componen.

Las propias empresas y el estado de debe crear conciencia sobre la importancia del cumplimiento de las Leyes de Protección de Datos Personales en todos los niveles organizativos, brindar las herramientas para que la misma facilidad que se tuvo de ingreso a una plataforma sea válida para salir de esta y que los datos ya no sean usados de una manera incorrecta. El ciudadano pueda editar, eliminar, cambiar los datos al tener el sustento necesario para rectificar algo erróneo, no hacer firmar acuerdos de confidencialidad que vulneren los derechos de intimidad y sigilo.

Tener un SGSI tomando como base la integridad, disponibilidad y confidencialidad, ayuda a mejorar los datos obtenidos de todas las personas sus controles conjuntamente con la ISO 27002 nos mencionan que se debería recabar de información y donde debemos tener cuidado. Otros países de la Unión Europea han logrado frenar a multinacionales a que los datos sean protegidos, en Latinoamérica países precursores como México, Chile y Argentina, sancionan a empresa por incumplimiento de las Leyes al darse cuenta que existe la fuga de información o

robo de bases de datos.

Garantizar que se obtenga un consentimiento adecuado para recopilar y procesar datos personales es el primer paso que la ciudadanía debe conocer, métodos de difusión existe, ejemplos de cómo se ha disminuido las incidencias de vulnerabilidad de datos se los encuentra, los SGSI de los diferentes países esclarecen como debe funcionar la de la normativa y el apoyo de Ecuador en mantener segura la data de los ciudadanos.

Conclusiones

La Ley de Protección de Datos vigente en Ecuador presenta todavía falencias dentro del COIP se debería más énfasis a los delitos informáticos, la forma que se sanciona y no solo a las empresas por el mal tratamiento de los datos personales, multas de cárcel es algo tradicional, pero al igual que en otros países se debería dar un seguimiento y privar de medios tecnológicos o acceso a quien realizo el delito, para iniciar con todo esto se debe categorizar la información en niveles de riesgo y criticidad.

Desde la parte judicial también se debe hacer estudios más profundos de que datos deberían ser resguardados muy bien por una entidad y que información no debería ser recopilada, los delegados de protección de datos en las empresas deben ser capacitados, tener en las instituciones por lo menos un oficial de seguridad de la información que ave que información no debería ser púbica, que información debe ser interna y cual se restringe, todo dato obtenido en muchos de los casos no tiene una base legal o sustento de porque se están recopilando los datos, con la nueva superintendencia de Ley de Protección de Datos la ciudadanía tiene expectativas grandes del trabajo conjunto que esta la debe realizar con instituciones de seguridad, telecomunicaciones y gubernamentales para la aplicación de la ley en el ciberespacio.

Este articulo también ofrece valiosos análisis donde se muestra los ataques más frecuentes que las empresas pueden tener y con tener la implementación de un buen sistema SGSI, con enfoque interdisciplinario que suman aspectos legales y tecnológicos muchas brechas encontradas se podrán subsanar, así como planes de riesgos y procesos dentro de las empresas que ayuden a que el negocio no se pierda por completo por un ataque informático.

Referencias bibliográficas

ANCI. (2021). *Resumen ciberataque que afectó a sistema aeronáutico provisto por SITA* (p. 7). https://anci.gob.cl/documents/217/10CND21-00047-01.pdf

ANT. (2021, octubre 21). *La ANT informa sobre un ataque cibernético a sus sistemas*. https://x.com/ANT_ECUADOR/status/1451247509557366795/photo/1

Argentina.gob.ar. (2023, junio 11). *La CNV aisló y controló un ataque informático*. https://www.argentina.gob.ar/noticias/la-cnv-aislo-y-controlo-un-ataque-informatico

AsambleaNacional. (2023). *Envío Informe para Primer Debate Ley Orgánica de Seguridad Digital* (Ley No. AN-CSIS-2023-0123-M). https://ppless.asambleanacional.gob.ec/alfresco/d/d/workspace/SpacesStore/63880065-2446-4048-8524-87541f88d84d/INFORME%20PARA%20PRIMER%20DEBATE.pdf

Balseca, D. (2024, julio 3). *Las 7 capas de CiberSeguridad en el Sector Financiero* [Sitios de noticias]. NGS Security Logic. https://www.ngs.com.ec/

Banco Mundial. (2021, octubre 23). *El bajo costo de cerrar la brecha digital en América Latina*. https://www.bancomundial.org/es/news/feature/2022/01/11/cerrar-brecha-digital-america-latina

Banco Pichincha. (2021, octubre 11). *Comunicado Oficial a Nuestros Clientes*. https://x.com/BancoPichincha/status/1447628963858296834/photo/1

Barrero, R. A. R., Vergara, V. Y. U., & Chaves, N. G. Z. (2023). *Impacto de la Inteligencia Artificial en la protección de datos en el sector financiero.*

CERT.ar. (2022). *El ransomware, el software malicioso usado para atacar a las organizaciones*.

CNT. (2021, julio 16). *La Corporación Nacional de Telecomunicaciones CNT EP a la opinión pública—CNT presentó denuncia ante la Fiscalía*. https://institucional.cnt.com.ec/noticias/la-corporacion-nacional-de-telecomunicaciones-cnt-ep-a-la-opinion-publica-cnt-presento-denuncia-ante-la-fiscalia

COE. (2022, marzo). *The Budapest Convention (ETS No. 185) and its Protocols* [Normas]. Consejo de Europa. https://www.coe.int/en/web/cybercrime/the-budapest-convention

CongresodelaUnion. (2017). *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* [Ley]. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

CSIRT.TELCONET. (2023, octubre 25). *Servicios Gubernamentales de Chile afectados por ataque de Ransomware*. https://csirt.telconet.net/comunicacion/noticias-seguridad/empresa-de-telecomunicaciones-que-sirve-al-gobierno-chileno-fue-victima-de-ataque-ransomware/

Diario Oficial UE. (2016). REGLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO - de 27 de abril de 2016—Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/ CE (Reglamento general de protección de datos). *REGLAMENTO (UE)*, *119*, 1-88.

ElPeruano. (2011). *REGLAMENTO DE LA LEY Nº LEY DE PROTECCIÓN DE DATOS PERSONALES* (Ley No. 29733). https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf?v=1618338779

Enríquez, L. (2021, junio 15). *La protección de datos en América latina: Influencia del RGPD*. https://www.uasb.edu.ec. https://www.uasb.edu.ec/ciberderechos/2021/06/15/la-proteccion-de-datos-en-america-latina-influencia-del-rgpd/

FGE. (s. f.). *Delitos informáticos en Ecuador* [Estatal]. https://www.fiscalia.gob.ec/

FuncionPublica. (2012). *LEY ESTATUTARIA 1581 DE 2012* [Ley]. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

GobiernoElectronico. (2023). *LEY ORGÁNICA PARA LA TRANSFORMACIÓN DIGITAL Y AUDIOVISUAL*. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2023/02/7e52b3d7-0ba5-4c58-a474-00e19fcbe127.pdf

González, A. M. V. (2024). *ATAQUES DE RANSOMWARE MÁS RELEVANTES EN LOS ÚLTIMOS CINCO AÑOS QUE HAN AFECTADO A LAS ORGANIZACIONES COLOMBIANAS*. UNAD.

Iñiquez, F. (2024, mayo 6). Perspectivas de la ciberseguridad nacional. *Estado actual de la ciberseguridad Ecuador 2024*. https://itahora.com/2024/05/06/perspectivas-de-la-ciberseguridad-nacional/

Jung, J., & Katz, R. (2023). *Impacto del COVID-19 en la digitalización de América Latina*.

KASEYA. (2021, julio 5). *Kaseya Responds Swiftly to Sophisticated Cyberattack*. https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/

Kasperky. (2023, agosto 30). *Empresas latinoamericanas reciben un promedio de dos ataques de ransomware por minuto, señala Kaspersky*. https://latam.kaspersky.com/about/press-releases/2023_empresas-latinoamericanas-reciben-un-promedio-

de-dos-ataques-de-ransomware-por-minuto-senala-kaspersky

Lexis. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES* (Ley No. T. 680-SGJ-21-0263). https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

LeyChile. (2023). *PROTECCION DE DATOS DE CARACTER PERSONAL* [Ley]. https://www.bcn.cl/leychile/navegar?idNorma=141599

Lezama, J., Ayala, L., Coulter, P., Wainberg, A., Moiraghi, S., Igarzabal, A., & Zamora, J. (2023, junio). MONITOR GEO. *Monitor GEO: Capítulo Nacional*, *255*, 32-37.

Marti, P. A., & Maciejewski, M. (2024, mayo). *La protección de los datos personales*. https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/es/FTU_4.2.8.pdf

MDMQ. (2022). *INFORME DE LA DIRECCIÓN METROPOLITANA DE INFORMÁTICA AL PLENO DEL CONCEJO METROPOLITANO DE QUITO* (Información sensible No. DMI-INF001-V2-CMQ; pp. 1-17). MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO. https://www7.quito.gob.ec/mdmq_ordenanzas/Administraci%C3%B3n%202019-2023/Sesiones%20de%20Concejo/2022/Sesi%C3%B3n%20216%20Ordinaria%202022-04-26/VI.%20DMI/DMI%20Informe%20al%20Pleno%20del%20Concejo%20Metropolitano%20de%20Quito%202022-ABR-28.pdf

MINTEL. (2022). *Estrategia Nacional de Ciberseguridad del Ecuador*. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf

MINTEL. (2024). *EXPÍDESE EL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN – EGSI QUE SE ENCUENTRA COMO ANEXO AL PRESENTE ACUERDO MINISTERIAL, EL CUAL ES EL MECANISMO PARA IMPLEMENTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR PÚBLICO* [Normas]. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2024/03/Registro-Oficial-Acuerdo-Ministerial-No.-0003-2024-EGSI-version-3.0.pdf

MINTIC. (2022, diciembre 16). *En el último mes y medio MinTIC ha recibido 36 reportes de ataques cibernéticos en Colombia* [Gubernamental]. https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/273464:En-el-ultimo-mes-y-medio-MinTIC-ha-recibido-36-reportes-de-ataques-ciberneticos-en-Colombia

MisiteriodeGobierno. (s. f.). *Delitos Informáticos en Ecuador* [Estatal]. https://www.ministeriodegobierno.gob.ec/

Novoa, E. (2020). El derecho a la protección de datos de personales en la prestación de servicios de cloud computing.: Una perspectiva ecuatoriana. *Revista de Derecho*, *22*, 64-89. https://doi.org/10.22235/rd22.2239

Ochoa, S. (2022). *Informe DMI sobre suceso informático de 16 de abril* (Informe Técnico No. Sesión Nº 55 de la Comisión de Conectividad; pp. 1-16). MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO. https://www7.quito.gob.ec/mdmq_ordenanzas/Administraci%C3%B3n%202019-2023/Sesiones%20de%20Concejo/2023/Sesi%C3%B3n%20265%20Ordinaria%202023-01-03/IV.%20Primer%20debate/Aportes/GADDMQ-SDPC-2022-0108/informe_conectividad_sesion_22_a.pdf

Planalto. (2018). *Lei Geral de Proteção de Dados Pessoais (LGPD)*. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

PrensarioTI. (2024, enero 2). Estudio de Kaspersky muestra la falta de conciencia sobre protección de datos en américa latina. *https://prensariotila.com*. https://prensariotila.com/estudio-de-kaspersky-muestra-la-falta-de-conciencia-sobre-proteccion-de-datos-en-america-latina/

RegistroOficial. (2023). *LEY ORGÁNICA REFORMATORIA A VARIOS CUERPOS LEGALES PARA EL FORTALECIMIENTO DE LAS CAPACIDADES INSTITUCIONALES Y LA SEGURIDAD INTEGRAL* [Ley]. https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/18400-suplemento-al-registro-oficial-no-279

RIPD. (2016). *Estandares de Protección de Datos Personales*.

Robles Osollo, A. G. (2021). El derecho a la privacidad y la protección de datos personales transfronterizos. *Revista Eurolatinoamericana de Derecho Administrativo*, *8*(1), 35-60. https://doi.org/10.14409/redoeda.v8i1.9543

Santamaría, F. (2020). El principio de responsabilidad proactiva: Una oportunidad para un mejor cumplimiento de la normativa en materia de protección de datos de carácter personal en el ámbito latinoamericano. *Derecho PUCP*, *85*, 139-174. https://doi.org/10.18800/derechopucp.202002.005

SB. (2021). *Acciones de la Super de Bancos frente a Ciberataque de entidad controlada*. https://www.superbancos.gob.ec/bancos/acciones-de-la-super-de-bancos-frente-a-ciberataque-de-entidad-controlada/

SEPS. (2022). *NORMA DE CONTROL RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO BAJO CONTROL DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA* (Normas Nos. 2022-002; p. 26). SEPS. https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf

SRI. (2021, julio 31). *BOLETÍN 018—INTEGRIDAD DE LOS SISTEMAS INFORMÁTICOS DEL SRI*. https://www.sri.gob.ec/boletines-2021. https://www.sri.gob.ec/o/sri-portlet-biblioteca-alfresco-internet/descargar/82296e08-9896-4e9a-bf43-b40b23711e53/BOLET%c3%8dN%20018%20-%20INTEGRIDAD%20DE%20LOS%20SISTEMAS%20INFORM%c3%81TICOS%20DEL%20SRI.pdf

SuperintendenciaDeBancos. (2021). *NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO* (Normas No. IX; pp. 1-34). https://www.superbancos.gob.ec/bancos/descargas/30300/