Polo del Conocimiento

Pol. Con. (Edición núm. 52) Vol. 5, No 11
Noviembre 2020, pp. 565-590
ISSN: 2550 - 682X
DOI: 10.23857/pc.v5i11. 2009

La tecnología y los riesgos sobre la privacidad y protección de datos

Technology and the risks of privacy and data protection

Tecnologia e os riscos da privacidade e proteção de dados

Diego Leonardo Loja-Molina [I]
dlojam@ucacue.edu.ec
https://orcid.org/0000-0002-4420-2208

Juan Cuenca-Tapia [II]
jcuenca@ucacue.edu.ec
https://orcid.org/0000-0001-5647-5150

Correspondencia: dlojam@ucacue.edu.ec

Ciencias Técnicas y Aplicadas
Artículo de investigación

*__Recibido:__ 20 de septiembre de 2020 *__Aceptado:__ 29 de octubre de 2020 __* Publicado:__ 25 de Noviembre de 2020

I. Ingeniero de Sistemas, Jefatura de Posgrados, Universidad Católica de Cuenca, Cuenca, Ecuador.

II. Magíster en Sistemas de Información Gerencial, Docente de la Unidad Académica de Tecnologías de la Información y Comunicación (TIC), Jefatura de Posgrados, Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

El presente artículo trata sobre los riesgos sobre la privacidad y protección de datos con el uso de la tecnología. El objetivo principal de esta investigación es la de exponer el cuidado y la importancia que se debe tener al momento de suministrar información personal ya que la misma puede ser utilizada para perjudicar a los afectados y por otro lado proporcionar beneficios a terceros como empresas que utilizan esa información para diferentes fines y/o venderlas a su vez a otras empresas que se encargan del procesamiento de datos. Aun en la actualizada, las personas no están muy conscientes de la magnitud que implica el registrar sus datos personales en un sitio web, pero, sin embargo, si prestaban atención a los portales o aplicaciones que les solicitan información acerca de sus cuentas bancarias, tarjetas de crédito/debito para realizar pedidos/compras o subscripciones a algún tipo de servicio de interés porque consideran que el patrimonio más importante para ellos es su capital (dinero) y por eso deben tener cuidado con ello, sin embargo, la información personal tiene un impacto más significativo del que se piense.

Palabras clave: Privacidad; protección; datos personales; riesgos; tecnología.

Abstract

This article deals with the risks to privacy and data protection with the use of technology. The main objective of this research is to expose the care and importance that must be taken when supplying personal information since it can be used to harm those affected and on the other hand provide benefits to third parties such as companies that use that information. information for different purposes and / or sell them in turn to other companies that are responsible for data processing. Even in the updated, people are not very aware of the magnitude involved in registering their personal data on a website, but, nevertheless, if they paid attention to the portals or applications that request information about their bank accounts, cards credit / debit to make orders / purchases or subscriptions to some type of service of interest because they consider that the most important asset for them is their capital (money) and that is why they should be careful with it, however, personal information has a more significant impact than you might think.

Keywords: Privacy; protection; personal data; risks; technology.

Resumo

Este artigo trata dos riscos à privacidade e à proteção de dados com o uso da tecnologia. O principal objetivo desta pesquisa é expor o cuidado e a importância que se deve ter no fornecimento de informações pessoais, uma vez que podem ser utilizadas para prejudicar os afetados e, por outro lado, proporcionar benefícios a terceiros, como as empresas que as utilizam. informações para diferentes fins e / ou vendê-las por sua vez a outras empresas responsáveis pelo processamento de dados. Mesmo na atualização, as pessoas não sabem muito bem a magnitude de registrar seus dados pessoais em um site, mas, mesmo assim, se prestaram atenção a portais ou aplicativos que solicitam informações sobre suas contas bancárias, cartões crédito / débito para fazer pedidos / compras ou subscrições de algum tipo de serviço de interesse porque consideram que o bem mais importante para eles é o seu capital (dinheiro) e por isso devem ter cuidado com ele, no entanto, as informações pessoais têm um impacto mais significativo do que você imagina.

Palavras-chave: Privacidade; proteção; dados pessoais; riscos; tecnologia.

Introducción

En la sociedad actual, la tecnología se encuentra involucrada en muchos aspectos de la vida diaria, las personas dependemos cada vez más en aspectos como las comunicaciones, transporte, educación, salud, entre otros. Actividades como la forma en la que se envían facturas, las consultas bancarias o la forma de pedir un taxi se ha transformado, ahora las empresas y los consumidores tiene acceso a información variada de manera inmediata 24/7.

El avance tecnológico no para y ha permitido que se desarrollen múltiples plataformas y servicios que a su vez se han convertido en canales de comunicación relevantes para ámbitos educativos, financieros, sociales, audiovisuales; por mencionar algunos en los que se han vuelto casi imprescindibles, las empresas ahora pueden prever el comportamiento de los consumidores con herramientas tecnológicas.

Distintos autores, entre los que destacan William J. Martin, considera que: “En la sociedad de la información, la calidad de vida, así como las perspectivas de cambio social y desarrollo económico dependen cada vez más de la información y su explotación” (Joel, 2001)

Ahora más que nunca la sociedad está enmarcada en la era digital, en donde su materia prima y actividades están estrechamente relacionadas a la tecnología, esto ha incrementado el ritmo de la

sociedad e implica el manejo de grandes volúmenes de información donde están incluidos los datos personales de los usuarios, por lo que mantener un control y contar con regulaciones en el manejo de estos datos resulta de vital importancia.

Para esto primeramente definimos los aspectos tecnológicos y su relación con los datos personales. Cuando hablamos de avances tecnológicos hacemos referencias a todos los recursos que usamos diariamente en la era digital los cuales usan la computación para tomar nuestros datos personales y almacenarlos en grandes volúmenes de información, por ejemplo:

- Motores de búsqueda: "Los buscadores o motores de búsqueda son sistemas que indexan los documentos de Internet sin seguir una estructura jerárquica como hacen los directorios. Este tipo de sistemas poseen unos programas especializados en recorrer la web de forma automática denominados crawlers (también llamados robots, spiders, wanderers, walkers o knowbots), que indexan los documentos que no contiene su base de datos" (Olivas Varela, 2011). Google con su conglomerado de servicios en la nube es el referente.
- **Plataformas digitales:** "son espacios en Internet que permiten la ejecución de diversas aplicaciones o programas en un mismo lugar para satisfacer distintas necesidades" (Giraldo, 2019), entre estas tenemos Spotify para música, Netflix para películas, Facebook para redes sociales, YouTube para videos, etc.
- **Inteligencia Artificial (IA):** "La Inteligencia Artificial es la parte de las Ciencias de la computación que se ocupa del diseño de sistemas de computación inteligentes, esto es, sistemas que exhiben las características que asociamos con la inteligencia en el comportamiento humano" (Barr & Feigenbaum, 1981).
- **Big Data:** "Macrodatos e inteligencia de datos son alternativas en español a la voz inglesa big data, que se emplea en el sector de las tecnologías de la información y de la comunicación (TIC) para aludir a un conjunto de datos que, por su volumen, variedad y velocidad de producción, no pueden ser analizados utilizando procesos o herramientas tradicionales" (Moreno-Carriles, 2018), existen productos basado en big data como Shazam para buscar contenido musical, Waze como herramienta de navegación en tiempo real.
- **Redes sociales:** "Las redes sociales se definen como estructuras en que los diferentes grupos mantienen relaciones sentimentales, amistosas o laborales en el contexto de la web 2.0, multiplicando los espacios de información, discusión e intercambio, de acuerdo con

preferencias, intereses, entre otros factores" (Izquierdo et al., 2017), mediante las cuales se pueden generar relaciones con empresas u otras personas sin barreras físicas y de manera más rápida.

- **IoT:** Por lo general, el término Internet de las Cosas se refiere a escenarios en los que la conectividad de red y la capacidad de cómputo se extienden a objetos, sensores y artículos de uso diario que habitualmente no se consideran computadoras, permitiendo que estos dispositivos generen, intercambien y consuman datos con una mínima intervención humana (Fedele & Fedele, 2011), se pueden usar aplicaciones para sistemas de seguridad, robótica, etc.
- **Blockchain:** en el texto se habla de Bitcoin (paradigma tecnológico conocido como Blockchain) "servidor de tiempo distribuido que identifica y ordena secuencialmente las transacciones e impide su modificación" (Monti & Rasmussen, 2017), utilizado en mercados como el de instituciones financieras pues generalmente se asocia con el Bitcoin y otras criptomonedas.

Todas estas herramientas permiten organizar la información, agilizar procesos, interactuar con otros usuarios e incluso generar modelos de negocios.

En cuanto a lo antes mencionado, el presente estudio pretende identificar los riesgos, perfilar los lineamientos que ayuden en el ejercicio de los derechos de los ciudadanos, relacionados con el uso de datos personales en las nuevas tecnologías. Con estos antecedentes, se buscan respuestas a las siguientes preguntas:

- ¿Qué piensan las personas alrededor del mundo sobre la privacidad y compartición de sus datos?
- ¿Cómo se encuentra América Latina en cuanto a marcos normativos y regulatorios?
- ¿Cuál es la situación del Ecuador respecto a la protección de datos?

Con los avances en la tecnología, el desarrollo y uso de sistemas informáticos para la manipulación de información en los aspectos de privacidad y protección de datos es cada vez más relevante para las personas que podrían ver comprometido este rol, tal es el caso del sistema de consultas del Consejo de la Judicatura, SATJE (Sistema Automático de Trámite Judicial Ecuatoriano), el cual es un sistema informático que registra y permite realizar un seguimiento de las actividades realizadas en cada una de las causas que se llevan en las diferentes Judicaturas, obteniendo información rápida y confiable en tiempo real (Judicatura, 2012).

Esta herramienta está dirigida a profesionales en Derecho de instituciones (públicas/privadas) y abogados en libre ejercicio para realizar trámites de manera virtual, entre las características del sistema están que permite subir archivos en formato PDF y de tipo multimedia (imágenes, audio), si el contenido a cargar excede cierto tamaño (peso en MB) se debe almacenar en ALFRESCO que es la plataforma para gestionar documentos superiores a 200 MB, ahí se deberá cargar mediante un servicio FTP para el cual se genera una dirección URL a la cual se debe acceder con las credenciales (usuario, contraseña) y cargar el archivo.

El proceso de consulta de causas web se lo puede realizar a través de su portal en el link: http://consultas.funcionjudicial.gob.ec/informacionjudicial/public/informacion.jsf, en donde se puede consultar un proceso por los datos de actor/ofendido y/o demandado/procesado, el número de proceso y numero de fiscalía, una vez ingresados los datos requeridos, en la parte inferior se mostrarán los resultados que coinciden con la búsqueda (fecha de ingreso, numero de proceso y acción/delito), para conocer más acerca de un proceso se debe acceder al detalle, posterior a esto el detalle muestra los movimientos del proceso, número de ingreso, fecha, los actores y demandados; también se puede conocer las actividades de cada proceso y a su vez exportarlas a un archivo en formato PDF.

Como se puede concluir del proceso de consulta descrito anteriormente, no se cuenta con un mecanismo de control y acceso a la información, está presente el objetivo de cumplir con el derecho a la información pública de las causas judiciales, sin embargo, esto podría vulnerar la tutela de otros derechos fundamentales y/o entrar en contradicción con otros derechos humanos.

La estructura y contenido del artículo se desarrolla de la siguiente manera: en la sección 2 se presentan conceptos relacionados con la investigación, en la sección 3 se establece fuentes bibliográficas de experiencias y resultados de investigaciones de privacidad y protección de datos. En la sección 4 se detalla la metodología utilizada para desplegar esta investigación. En la sección 5 se presentan los resultados relacionados a la privacidad y protección de datos en el Ecuador. Por último, en la sección 6 se establecen las conclusiones de acuerdo con los resultados obtenidos.

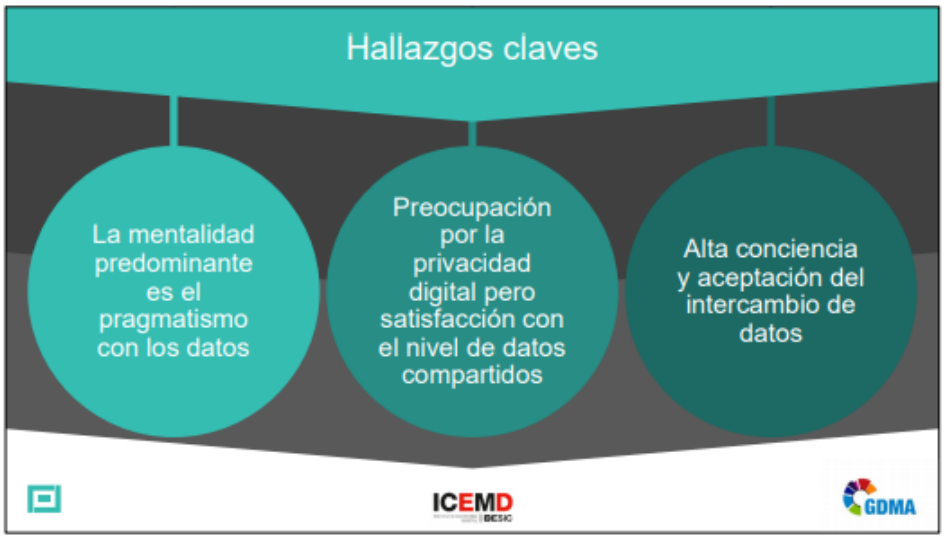
Desarrollo

Trabajos relacionados

Tras un estudio impulsado en España por ICEMD encargado por la Global Alliance of Data-Driven Marketing Associations (GDMA) 2018, en una encuesta digital realizada a 11.474 personas mayores de 18 años de países como: Estados Unidos, España, Australia, Canadá, Singapur, Reino Unido, Alemania, Francia, Países Bajos y Argentina; demostró que consumidores alrededor del mundo ha adoptado enfoques pragmáticos (práctica), fundamentalistas y despreocupados al momento de compartir su información personal, esto a pesar de ciertos aspectos como las diferencias sociales, culturales y económicas (Privacidad de Datos En El Mundo : Lo Que Realmente Piensan Los Consumidores, n.d.).

También, otros resultados importantes del estudio permitieron determinar ciertos hallazgos claves los cuales permiten apreciar que la mentalidad pragmática es predominante con respecto a compartir la información personal, también otro hallazgo es una cierta preocupación por la privacidad, pero sin embargo una satisfacción sobre los datos compartidos y el último hallazgo es que existe conciencia y aceptación en cuanto al intercambio de datos.

Figura 1: Hallazgos clave encuesta ICEMD (GSMA) 2018.



Fuente: Encuesta ICEMD (GSMA) 2018.

Este estudio demuestra que la mayoría de las personas (51%) realizada en 10 países y 4 continentes encuestados decidirán si comparten su información personal (caso por caso) en función de los

beneficios que pudieren obtener, otro porcentaje (23%) manifiesta no proporcionar ningún tipo de información personal a pesar de que exista algún beneficio presente y otro grupo (26%) de individuos a quienes no le preocupa la recopilación y uso de su información personal (Privacidad de Datos En El Mundo : Lo Que Realmente Piensan Los Consumidores, n.d.).

Figura 2: Pragmatismo es la mentalidad predominante ICEMD (GSMA) 2018.

Fuente: Encuesta ICEMD (GSMA) 2018.

Sin lugar a dudas, las situaciones particulares de este fenómeno se dan cuando se producen una divulgación de datos, es entonces donde se entiende realmente el problema, la posición que representa perder la privacidad y las consecuencias que con lleva, esto no significa que los usuarios no posean responsabilidad sobre sus datos, al contrario, deben poseer la capacidad de proteger su privacidad al cuestionar sobre la cantidad de datos solicitantes y decidir qué cantidad de datos entregar.

Con respecto a los derechos y responsabilidades de las personas en cuanto a la seguridad de su información personal los resultados del estudio señalan que una media del 38% de individuos dicen que las propias personas deben ser responsables de la seguridad de sus datos, un 15% indica que los gobierno a través de sus instituciones deberían encargarse, mientras que un 5% dice que las empresas u organizaciones lo deben hacer, el estudio también expone en un 35% que la

responsabilidad debería ser resultado de la combinación de todas estas alternativas (Privacidad de Datos En El Mundo : Lo Que Realmente Piensan Los Consumidores, n.d.).

Figura 3: Derechos y responsabilidades ICEMD (GSMA) 2018.

Fuente: Encuesta ICEMD (GSMA) 2018.

Basado en los resultados del estudio se puede decir que la privacidad se vuelve colectiva porque nos exhibe y también a los demás, por lo que proteger nuestra privacidad se convierte en un esfuerzo colectivo en donde es necesario tomar medidas como la de exigir sanciones contra empresas irresponsables que divulguen información y de cualquier riesgo que se presente en esta era en donde el consentimiento resulta ser uno de los problemas más graves de la ética digital.

Una investigación realizada por la Comisión Interamericana de Telecomunicaciones (CITEL) 2019 y liderada por Gianncarlo Gomez Morales acerca del estado de la protección de datos en América Latina revelo que existe un nivel de madurez en cuanto a la implementación de marcos regulatorios y normativos en la región, en donde Perú sobre sale siendo uno de los países que cuenta una ley que regula la protección de la información de manera meticulosa (ESAN, 2019).

Para esta investigación el CITEL evaluó criterios como: registros nacionales, habeas data, la legislación de los países y los departamentos involucrados en el área de la ciberseguridad, los resultados se pueden apreciar a continuación:

Figura 4: Niveles de madurez en la normatividad relacionada a la protección de Datos Personales en los países de la región (CITEL) 2019.

Nº	PAIS	No tiene Ley	Habeas Data	Ley Aprobada	Autoridad nacional de protección y/o supervisión	Registro nacional de bancos de datos personales	Nivel de madurez	Comentario
1	ARGENTINA		X	X	X	X	OPTIMIZADO	
2	BOLIVIA		X				INICIADO	
3	BRASIL		X				INICIADO	
4	CANADÁ			X	X		GESTIONADO-	SIN HABEAS DATA
5	CHILE		X	X		X	OPTIMIZADO-	SIN AUTORIDAD NACIONAL
6	COLOMBIA		X	X	X	X	OPTIMIZADO	
7	COSTA RICA		X	X	X	X	OPTIMIZADO	
8	ECUADOR		X	X		X	OPTIMIZADO-	SIN AUTORIDAD NACIONAL
9	EL SALVADOR	X					INEXISTENTE	
10	ESTADOS UNIDOS		X	X	X		GESTIONADO	
11	GUATEMALA		X				INICIADO	
12	MEXICO		X	X	X	X	OPTIMIZADO	
13	PANAMA	X					INEXISTENTE	
14	PERU		X	X	X	X	OPTIMIZADO	
15	PARAGUAY		X	X			DEFINIDO	
16	REPUBLICA DOMINICANA		X	X			DEFINIDO	
17	URUGUAY		X	X	X	X	OPTIMIZADO	
18	VENEZUELA			X			DEFINIDO-	SIN HABEAS DATA

Fuente: Gianncarlo Gomez Morales 2019.

Con estos aspectos presentes en la investigación se puede apreciar que existen países que no cuenta con una ley como Panamá y El Salvador por lo que no tiene ningún nivel de protección. También se puede ver que existen países que tienen un nivel de madurez definido (República Dominicana, Paraguay y Venezuela). Países como Argentina, Chile, Colombia, Costa Rica, México, Perú y Uruguay tienen un nivel de madurez optimizado (cuentan con leyes requeridas en los criterios evaluados por el CITEL) (ESAN, 2019).

Metodología

A continuación, se describen los pasos utilizados en esta investigación:

- **Reglamento General de Protección de Datos:** normativa vigente de la UE (Unión Europea), encargado y referente mundial con respecto al tratamiento y circulación de datos.
- **Marco Jurídico en el Ecuador:** se describen las leyes que se han establecido para el control y regulación de privacidad y protección de datos en el Ecuador.
- **Casos relacionados a la privacidad y protección de datos:** se conocen los casos relevantes relacionados a la privacidad y protección de datos los cuales han generado polémica y a su vez ha permitido adoptar medidas correctivas.

- **Búsqueda y selección de portales que exponga información personal:** buscar portales web que procesen, almacenen o exhiban información personal sin métodos de acceso restringido o algún tipo de seguridad.
- **Aspectos jurídicos y técnicos (seguridad) de portales evaluados:** a partir del uso del portal se obtuvo como resultado que el mismo podría vulnerar ciertos aspectos jurídicos y carecer de buenas prácticas, estándares y normas que se contemplan para el manejo de datos personal lo cual compromete la información que almacenan.

Resultados

Reglamento General de Protección de Datos

El RGPD, Reglamento General de Protección de Datos, es una ley europea de protección de datos que fue aprobada el 27 de abril de 2016, pero a partir de mayo de 2018 se aplicó para los estados miembros de la UE (Unión Europea) el cual busca dar control sobre sus datos personales.

Este reglamento aspira regular el derecho a la privacidad y tiene como objetivo la protección de los datos, los derechos y libertades físicas de las personas en respecto al procesamiento de la información personal.

Tal como lo expone Susan Chen (2010) en privacidad y protección de datos: “Los principios generales son esenciales para garantizar, en forma directa, la adecuada protección de la información personal (y, en algunos casos, los intereses legítimos de personas jurídicas), e indirectamente, para salvaguardar los derechos a la privacidad, al honor, a la reputación, a la libertad de expresión (incluyendo la libertad de prensa), entre otros; mediante la generación de un adecuado marco jurídico en donde puedan hacerse efectivos todos y cada uno de estos derechos y garantías fundamentales del hombre” (Universidad de Costa Rica. Escuela de Historia & Alpízar, 2010)

Los datos que fueron adquiridos por las necesidades del giro del negocio debe obedecer a políticas y/o normativas sustentadas y legalmente aprobadas, siendo estas intransferibles bajo ninguna figura y conservadas bajo la misma estructura de seguridad, almacenamiento e integridad. Con este antecedente, se hace énfasis en ciertas consideraciones principales que las empresas deben tener en cuenta para la adopción del Reglamento General de Protección de Datos (RGPD) (Union Europea, 2018):

- La verificación de datos
- Informar sobre la verificación de datos

- Conservar los datos necesarios
- Protección de los datos
- Histórico sobre actividades del uso de datos
- Contratos de confidencialidad
- Cumplimiento de disposiciones

Marco Jurídico en el Ecuador

Para esta sección se recurrió al Marco Jurídico en el Ecuador tomando con referencia el Reglamento General de Protección de Datos con sus estatutos, actores y roles que controlan y regulan la información personal, la información ha sido extraída del Proyecto de Ley Orgánica de Protección de Datos Personales, 2019. Se ha tomado en cuenta los conceptos de:

- Datos personales
- Encargado del tratamiento de datos personales.
- Responsable de tratamiento de datos personales.
- Seguridad y confidencialidad de datos personales.
- Transferencia de datos a terceros.
- La autoridad y protección de los datos personales.

Datos Personales

Datos personales: “Dato que identifica o hace identificable a una persona natural, directa o indirectamente, en el presente o futuro. Los datos inocuos, metadatos o fragmento de datos que identifiquen o hagan identificable a un ser humano, forman parte de este concepto” (Ecuador, 2019). Art. 4. (6)

Encargado del tratamiento de datos personales

Encargado del tratamiento de datos personales: “Persona que trate datos personales por nombre y a cuenta de un responsable de tratamiento de datos personales”. (Ecuador, 2019). Art. 4. (13)

Responsable del tratamiento de datos personales

Responsable del tratamiento de la información: “Persona natural o jurídica, pública o privada que decide sobre la finalidad y tratamiento de datos personales” (Ecuador, 2019). Art. 4. (18)

Seguridad y confidencialidad de datos personales

Seguridad de datos personales: "El responsable o encargado del tratamiento de datos personales. según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta el estado de la técnica, mejores prácticas de segundad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos y el nivel de impacto que estos representen a los derechos fundamentales y libertades individuales" (Ecuador, 2019). Art. 50.

El documento expresa que el encargado o responsable del tratamiento de datos personales habrá de implementar procesos para la revisión, evaluación y valoración de aspectos de carácter organizativo, técnico u otra índole que garanticen y mejoren la seguridad y tratamiento de datos personales.

El proyecto de ley también considera en su Art.50 que el encargado o responsable del tratamiento de datos personales demostrará que las medidas acogidas e implementadas mitiguen los riesgos identificados adecuadamente, entre estas medidas se puede incluir las siguientes:

1. Medidas de anonimización, encriptación, cifrado o codificación de datos personales;
2. Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes; y,
3. Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, organizativa, y jurídica.

Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares para medición y gestión de riesgos, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales (Ecuador, 2019). Art. 50.

Transferencia de datos a terceros países

Transferencia o comunicación internacional de datos personales: "La transferencia o comunicación internacional de datos personales será posible si se sujeta a lo previsto en el presente capítulo, la presente Ley o la normativa especializada en la materia, propendiendo siempre al efectivo ejercicio del derecho a la protección de datos personales". (Ecuador, 2019). Art. 64.

La autoridad y protección de los datos personales

Autoridad de Protección de Datos Personales: el proyecto de ley en su Artículo 88 dice: "La Autoridad de Protección de Datos Personales será una entidad de derecho público dependiente del Función Ejecutiva con personería jurídica y gozará de autonomía administrativa y financiera". (Ecuador, 2019). Art. 88.

Tabla 1: Estado Normativas en Ecuador frente al RGPD.

Marco Normativo	Unión Europea	Ecuador
Datos personales	✔	✔
Encargado del tratamiento de datos personales	✔	✔
Responsable del tratamiento de datos personales	✔	✔
Seguridad y confidencialidad de datos personales	✔	✔
Transferencia de datos a terceros países	✔	✔
La autoridad y protección de los datos personales	✔	✔

Fuente: Elaboración propia.

Casos relacionados a la privacidad y protección de datos

Caso privacidad de datos

La privacidad nos provee una zona (metafórica) de seguridad, lastimosamente no siempre pensamos que el principio de privacidad sea importante y no entendemos o no reflexionamos porque deberíamos protegerla. En la actualidad, este conjunto de datos se distribuye, estudian y utilizan en procesos de marketing, para publicidad y gestión de recursos humanos.

Sobre lo anterior, basta con recordar lo ocurrido con Cambridge Analytica (2018) en que la empresa se vio involucrada en un escándalo después de que un ex-empleado revelara algunas prácticas de la compañía para influir en elecciones políticas en la cual se usaron datos personales para manipular elecciones.

Cambridge Analytica fue una empresa privada de análisis de datos en redes sociales que decía permitir mover la perspectiva humana en ciertos tópicos específicos a través del uso de Big Data y Machine Learning, se auto identificaba como el poder del Big Data y los análisis psicográficos en los procesos de elecciones. (Oriza, 2018)

Mediante una aplicación que aparentemente era inofensiva (Thisisyourdigitallife) Cambridge Analytica pago en 2013 a 270.000 usuarios para hicieran un supuesto test de personalidad, de esta manera accedieron a los datos de estos usuarios y también a los datos de sus amigos, es decir, accedieron al grafo social de los usuarios de Facebook. (González, 2018)

Cabe mencionar que Cambridge Analytica básicamente tuvo acceso a toda la información que fuese accesible de los perfiles que usaron la aplicación (tanto de los que permitieron el acceso como lo que no), entre esto se incluye información como: intereses, fotografías, publicaciones, religión, cumpleaños, estado sentimental, "me gusta", localización, etc., con lo cual se podrían crear patrones psicológicos con mayor exactitud.

Con esto, Cambridge Analytica obtuvo acceso a los datos de 87 millones de personas sin permiso de estas personas y los utilizaron para hacer micro-targeting (estudio del público objetivo o segmentación) especial e influenciar sobre la decisión de los usuarios indecisos o vulnerables para que fuesen objetos de anuncios o noticias falsas con la finalidad de encaminarlos hacia un candidato y de esta manera afectar las elecciones en los Estados Unidos. (Arteaga, 2018)

Caso protección de datos

La Legislación Ecuatoriana contempla la protección de datos personales dentro de La Ley Orgánica de la Gestión de la Identidad y Datos Civiles, Artículo 1 objeto la cual manifiesta "La presente Ley tiene por objeto garantizar el derecho a la identidad de las personas y normar y regular la gestión y el registro de los hechos y actos relativos al estado civil de las personas y su identificación" (De et al., 2016).

A pesar de esto, la protección de datos personales en el Ecuador posee una regulación dispersa, tanto con el manejo de datos como el acceso a las redes pues no están normadas, lo cual demuestra que no se tiene una perspectiva hacia las tecnologías de la información y sus nuevos desafíos, también causa que las empresas que tratan con datos personales no ponen límites en su tratamiento, más bien hacen que obedezcan a sus intereses.

Con respecto a esto basta señalar la filtración de datos de Ecuador (2019) en donde la empresa de seguridad informática vpnMentor aseguró en un informe que el servidor que contenía la información personal de cerca de 17 millones de ecuatorianos no contaba con los protocolos necesarios de protección, (BBC News Mundo, 2019).

El ECUCERT (Centro de respuesta a incidentes informáticos del Ecuador) ha restringido el accesos a la base de datos que se encontraba en un servidor en Florida (Miami) administrado por la empresa

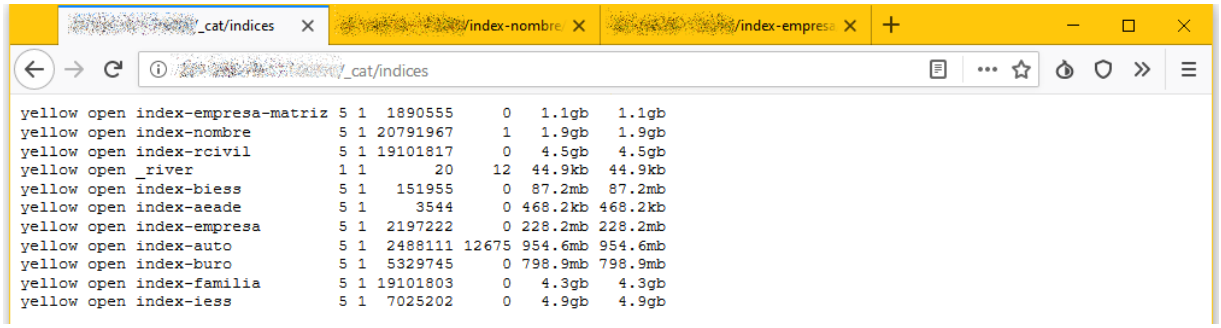
Novaestrat (empresa ecuatoriana de marketing y análisis), esta filtración de produjo por la mala configuración de un sistema llamado ELASTICSEASH (software de código abierto) que permite crear motores de búsqueda muy profundo, La base de datos estaba actualizada que incluía cerca de 6.7 millones de niños incluso de recién nacidos y contenía información reciente en 2019 (alrededor de marzo – abril de 2019).

De acuerdo a la revista Forbes los datos que se filtraron son los siguientes (Winder, 2019): nombre completo (nombre y apellidos), género, fecha de nacimiento, lugar de nacimiento, dirección de casa, dirección de correo electrónico, números de teléfono de casa, trabajo y celular, estado civil, fecha de matrimonio, fecha de fallecimiento, nivel de educación, nombre del empleador, ubicación del empleador, número de identificación fiscal del empleador, título profesional, información salarial, fecha de inicio del trabajo y fecha de finalización del trabajo.

Incluso si una persona tenía una cuenta bancaria con el BIESS (Banco del Instituto Ecuatoriano de Seguridad Social), incluía la siguiente información adicional como: estado de la cuenta, saldo actual en la cuenta, monto financiado, tipo de crédito, es decir, se podía acceder a la situación financiera de los ecuatorianos.

En cuanto a que cómo se encontraba la información en la base de datos, esta se presentaba como un sistema de búsqueda abierto formateado en CSV (valores separados por comas) y JASON (Notación de Objetos de JavaScript) el cual contaba con varios índices como información sobre la familia, datos de registro civil, información financiera y laboral, pero también datos sobre la propiedad del automóvil menciona ZDNet (Cimpanu, 2019), se puede apreciar los índices de la información de la base de datos a continuación:

Figura 5: Datos distribuidos en diferentes índices de Elasticsearch.



Fuente: ZDNet, 2019.

Pol. Con. (Edición núm. 52) Vol. 5, No 11, Noviembre 2020, pp. 565-590, ISSN: 2550 - 682X

Con respecto a lo tipos de datos se puede apreciar una estructura como la siguiente:

Figura 6: Datos de fuentes gubernamentales.


```
hits:
  0:
    _index:                    "index-rcivil"
    _type:                     "type-rcivil"
    _id:                       "[redacted]"
    _score:                    6.287284
    _source:
      cedula:                  "[redacted]"
      nombre_apellido:         "MORENO GARCES LENIN BOLTAIRE"
      cod_sexo:                "1"
      sexo:                    "Masculino"
      lugar_inscrip_nacimiento: ""
      fecha_nacimiento:        "[redacted]"
      lugar_nacimiento:        "[redacted]"
      codigo_nacionalidad:     "239"
      codigo_estado_civil:     "2"
      estado_civil:            "Casado/a"
      fecha_matrimonio:        "1975-07-29"
      codigo_domicilio:        "[redacted]"
      calle_domicilio:         "[redacted]"
      numero_casa:             "[redacted]"
      fecha_inscrip_defuncion: ""
      lugar_inscrip_defuncion: "0"
      fecha_defuncion:         ""
      fallecido:               "NO"
      codigo_instruccion:      "SUPERIOR"
      codigo_profesion:        "EMPLEADO PARTICULAR"
```


Fuente: ZDNet, 2019.

Búsqueda y selección de portales que exponga información personal

En cuanto a la búsqueda y selección de portales que provean información se ha tomado en cuenta de manera particular a las correspondientes a entidades públicas, que amparadas en La Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) la cual en su Artículo 1 expresa: “Principio de Publicidad de la Información Pública.- El acceso a la información pública es un derecho de las personas que garantiza el Estado” (Consejo para la Transparencia, 2013), y la que contempla en su Artículo 3 Ámbito de Aplicación de la Ley literal a) “Los organismos y entidades que conforman el sector público en los términos del artículo 118 de la Constitución Política de la República;” (Consejo para la Transparencia, 2013).

Siendo el Consejo de la Judicatura una entidad pública que almacena y manipulan información a través de la herramienta SATJE (Sistema Automático de Trámite Judicial Ecuatoriano) y que a su

vez manejan información sensible relacionado a la situación judicial/civil (casos, juicios, tramites, etc.) se ha seleccionado como potencial candidato.

A su vez, el portal de consultas del Consejo de la judicatura (SATJE) catalogado como herramienta tecnológica para gestionar los trámites judiciales en línea, tiene como a su vez lineamientos de su razón de ser debido a que: "Fundamentados en las necesidades institucionales se define a la Gestión Documental para el Consejo de la Judicatura, como el proceso automatizado que contribuye a la reducción de papel, optimización de tiempo en el flujo documental, almacenamiento, búsqueda, recuperación y distribución de documentos físicos y digitales, mediante herramientas tecnológicas que garanticen la creación, atención, distribución, respuesta, confidencialidad y acceso a la información generada desde y para el Consejo de la Judicatura y sus órganos desconcentrados" (Flores et al., 2017)

Esta herramienta permite a profesionales en Derecho de instituciones (publicas/privadas) y abogados en libre ejercicio realizar trámites de manera virtual, también en el sitio se puede consultar las causas web que son consultas de los procesos judiciales por su estado y actividades.

Si bien el manual de usuario del sistema indica en su contenido que existe un inicio de sesión destinado a los funcionarios del Consejo de la Judicatura para que puedan registrar trámites, no sucede de igual manera para la consulta por parte de usuarios externos lo cual está contemplada en la LOTAIP con el objeto de cumplir con el derecho a la información pública de causas judiciales.

Esto a su vez podría vulnerar otros derechos y generar problemas relacionados a la privacidad de la información que no cumple el sistema, pues si bien la información debe ser publica, esto transgrede situaciones como: casos de menores involucrados directa o indirectamente, situaciones de pensión alimenticia, cuando se ha cumplido la condena o casos simples como contravenciones que cualquiera persona puede consultar.

Aspectos jurídicos y técnicos de portales evaluados

Aspectos jurídicos

Con respecto a los aspectos jurídicos del portal evaluado que inicio como un proceso de automatización de tramites con el objeto de "Implementar una herramienta informática que reduzca la utilización de papel y automatice el flujo documental, mediante el uso del sistema de gestión documental entre las dependencias, unidades administrativas, direcciones provinciales y

direcciones nacionales del Consejo de la Judicatura" (Flores et al., 2017), pero el mismo podría vulneran aspectos relacionados a derechos humanos fundamentales como el derecho a la honra, al honor, a la intimidad, publicidad procesal, al buen nombre, a la integridad, independencia e imparcialidad y el derecho al olvido.

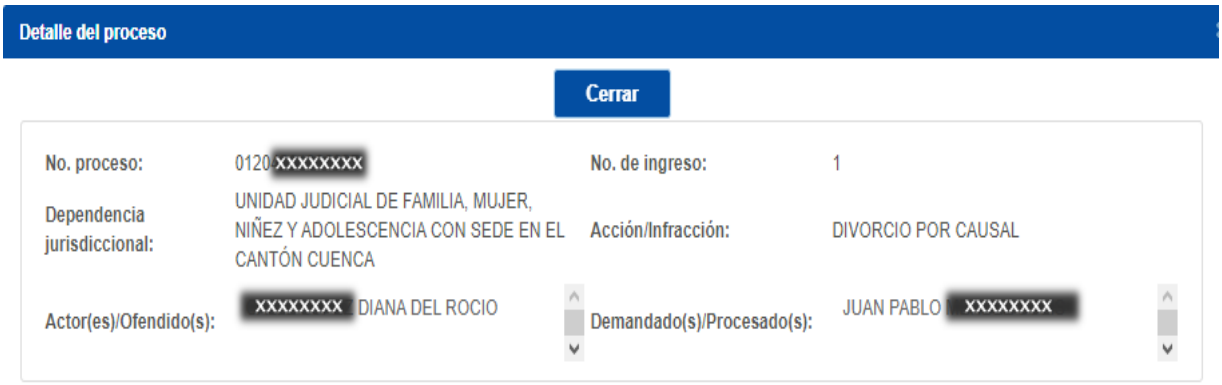
Cabe mencionar que efectivamente no existe un límite para los usuarios externos del sistema de consultas SATJE que muchas veces exponen información sensible en donde se ven involucrados derechos de NNA (niños, niñas y adolescentes), casos de violencia intrafamiliar, o temas como infracciones de tránsito donde sin que exista sentencia la persona es catalogada como presunta infractora, estos aspectos son los que desde el punto de vista jurídico y legal se puede tratar, claro, sin olvidar que existen derechos consagrados como el derecho a la información y publicidad de los procesos, sin embargo, se debería establecer hasta qué punto se garantiza este derecho procesal y constitucionalmente reconocido cuando puede existir incluso vulnerados derechos de grupos de atención prioritaria.

Un aspecto que se deriva de ciertas situaciones (como el cumplimiento de una condena) es que, con la factibilidad de acceso y consulta del portal sobre los datos de un individuo, éste fácilmente se puede convertir en una herramienta discriminatoria utilizada por la gestión de recursos humanos en una empresa al momento de calificar y/o aceptar personal, todo esto debido a que la información permanece expuesta, esto se considera una vulneración al derecho al olvido, el cual está relacionado con la protección de datos personales y el habeas data, derecho a la intimidad, la imagen, el honor y la honra.

A continuación, se presentan el resultado de una búsqueda realizada en el portal en la cual se puede apreciar cómo se presenta lo antes mencionado, aunque la fuente de la información fue obtenida del portal de consultas SATJE se han modificado las áreas que contiene la información de las partes involucradas en función de preservar el derecho a la intimidad y además por tratarse de un proceso en el cual está de por medio un menor de edad.

Para su conocimiento, se muestra una captura principal y capturas de partes del proceso ocultando por supuesto la identidad de los implicados en donde se intenta demostrar que se ha violado la confidencialidad de los datos. La información del proceso es la siguiente:

Figura 7: Detalle del proceso (Consejo de la Judicatura).



Detalle del proceso

Cerrar

No. proceso:	0120[redacted]	No. de ingreso:	1
Dependencia jurisdiccional:	UNIDAD JUDICIAL DE FAMILIA, MUJER, NIÑEZ Y ADOLESCENCIA CON SEDE EN EL CANTÓN CUENCA	Acción/Infracción:	DIVORCIO POR CAUSAL
Actor(es)/Ofendido(s):	[redacted] DIANA DEL ROCIO	Demandado(s)/Procesado(s):	JUAN PABLO [redacted]

Fuente: SATJE - Elaboración propia.

Figura 8: Sentencia y resumen (Consejo de la Judicatura).

SENTENCIA Y/O RESOLUCION

Juicio N.- 0120[redacted]

JUEZA PONENTE: DRA. SANDRA [redacted], Jueza de la Unidad Judicial de Familia Mujer, Niñez y Adolescencia de Cuenca.

MATERIA: DIVORCIO CAUSAL

PROCEDIMEINTO: SUMARIO

PARTES PROCESALES: DIANA DEL ROCIO [redacted] contra JUAN PABLO [redacted]

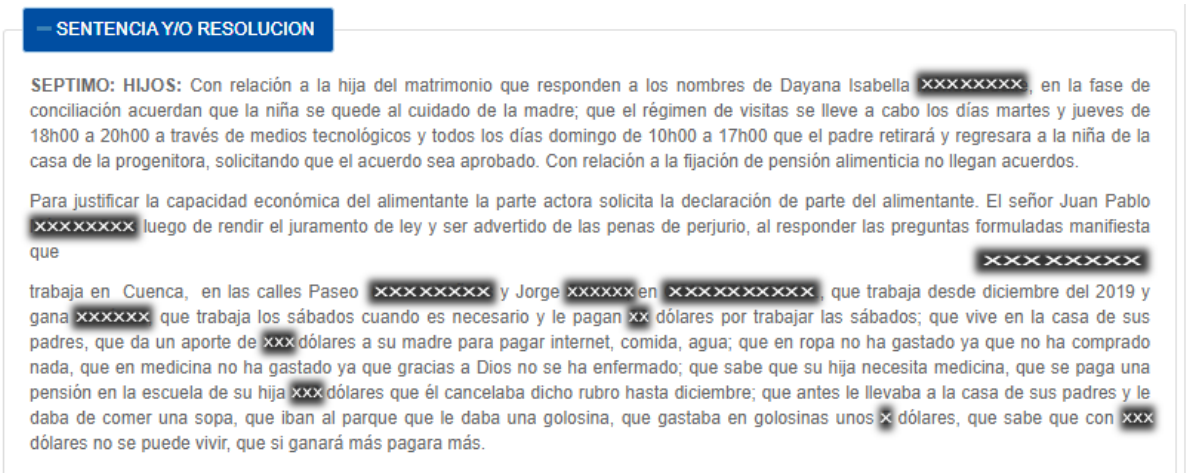
VISTOS: Cumpliendo con la obligación establecida en el Artículo 75 de la Constitución de la República del Ecuador, de conformidad con el artículo 90 del Código Orgánico General de Procesos, considerando que es base esencial de la Seguridad Jurídica y derecho Constitucional de las partes que requieren la intervención del órgano judicial; emite de conformidad con lo que dispone el Articulo 76 numeral 7 literal l de la Constitución la presente Resolución motivada, habiéndose evacuado la audiencia de juicio oral y pública dentro de la presente causa, y habiendo sido legalmente notificadas las partes con la resolución dada a conocer en forma oral, correspondiendo hacerlo por escrito se lo hace en los siguientes términos:

1.- ENUNCIACION BREVE DE LOS HECHOS Y CIRCUNSTANCIAS:

Comparece la señora Diana del Rocío [redacted] cuyo estado y condición constan de autos y manifiesta que se encuentra casado con el señor Juan Pablo [redacted] conforme inscripción de matrimonio que acompaña; que durante el patrimonio no han adquirido bienes inmuebles, solo lo necesario para la supervivencia de la familia; que3 han procreado una hija de cinco años de edad de nombres Dayanna Isabella [redacted] que desde hace aproximadamente a la fecha en su vida matrimonial han tenido constantes y habituales discusiones que se han agudizado en los últimos tres meses, que el 20 de septiembre del año en curso la situación fue insostenible llegando agresiones verbales como físicas lo que hizo que él salga de la casa pero se ha visto perseguida que acudido a la Junta Cantonal de Protección de derechos para que se le otorgue una boleta de auxilio para su protección y la de su familia. Que la falta de armonía en el hogar era evidente y no permitía llevar una vida plena de pareja y compartir sus vidas juntas a lado de su hija. Por lo que con fundamento en el Art. 110 numeral 3 del código Civil demanda en procedimiento sumario el divorcio a su cónyuge, solicita se declare con lugar la demanda y se disponga su marginación; anuncia medios de prueba documental y testimonial. Aceptada a trámite la demanda se dispuso citar al demando, que se dote de curador ad-litem a la hija del matrimonio, se ha fijado pensión provisional.

Fuente: SATJE - Elaboración propia.

Figura 9: Resolución Séptimo: Hijos (Consejo de la Judicatura).



SENTENCIA Y/O RESOLUCION

SEPTIMO: HIJOS: Con relación a la hija del matrimonio que responden a los nombres de Dayana Isabella xxxxxxxx, en la fase de conciliación acuerdan que la niña se quede al cuidado de la madre; que el régimen de visitas se lleve a cabo los días martes y jueves de 18h00 a 20h00 a través de medios tecnológicos y todos los días domingo de 10h00 a 17h00 que el padre retirará y regresara a la niña de la casa de la progenitora, solicitando que el acuerdo sea aprobado. Con relación a la fijación de pensión alimenticia no llegan acuerdos.

Para justificar la capacidad económica del alimentante la parte actora solicita la declaración de parte del alimentante. El señor Juan Pablo xxxxxxxx luego de rendir el juramento de ley y ser advertido de las penas de perjurio, al responder las preguntas formuladas manifiesta que xxxxxxxxx trabaja en Cuenca, en las calles Paseo xxxxxxxx y Jorge xxxxxx en xxxxxxxxxx, que trabaja desde diciembre del 2019 y gana xxxxxx que trabaja los sábados cuando es necesario y le pagan xx dólares por trabajar las sábados; que vive en la casa de sus padres, que da un aporte de xxx dólares a su madre para pagar internet, comida, agua; que en ropa no ha gastado ya que no ha comprado nada, que en medicina no ha gastado ya que gracias a Dios no se ha enfermado; que sabe que su hija necesita medicina, que se paga una pensión en la escuela de su hija xxx dólares que él cancelaba dicho rubro hasta diciembre; que antes le llevaba a la casa de sus padres y le daba de comer una sopa, que iban al parque que le daba una golosina, que gastaba en golosinas unos x dólares, que sabe que con xxx dólares no se puede vivir, que si ganará más pagara más.

Fuente: SATJE - Elaboración propia.

Aspectos técnicos

En cuanto a los aspectos técnicos o de seguridad del portal evaluado se puede proponer aquellos enfocados a un modelo AAA (Autenticación, Autorización y Auditoría) el cual es el modelo líder para el control de acceso y que en conjunto son usados para la protección y confidencialidad de la información.

El modelo AAA es considerado como una buena práctica de seguridad y que tiene como objetivo una gestión eficiente de los requisitos de seguridad la cual puede considerar su implementación para sistemas externos que consuman servicios web XML (Lenguaje de Marcado Extensible) utilizando WSDL (Lenguaje de Descripción de Servicios Web) desarrollado a partir de tecnologías libres, que sean multiplataforma y sobre arquitectura de capas utilizando cualquier framework que implemente un patrón de arquitectura Modelo-Vista-Controlador (MVC) además del uso de la metodología AJAX (JavaScript asíncrono y XML) para generar peticiones más eficientes hacia el servidor. (Morales & Karel Gomez Velázquez, Danisbel Rojas Rios, 2009)

La implementación del modelo AAA en cuanto a las consultas que pueden realizar los usuarios en el portal no solo generaría un nivel de seguridad al sitio sino también favorecería a poder controlar el acceso a la información. Para ello el modelo AAA utiliza en primera instancia el mecanismo de Autenticación que garantiza la identidad del usuario que desea ingresar (validar que corresponda quien dice ser), esta validación se realiza a través de sus credenciales (usuario y contraseña), luego se aplica el mecanismo de Autorización el cual otorga el nivel de acceso y la asignación de recursos basado en el perfil que el usuario tenga establecido, y por último el mecanismo de Auditoria que

cuenta con el registro de las actividades del usuario que ingreso al sistema, esto permite saber quién accedió, a que accedió y el tiempo.

El modelo AAA también se complementa con aspectos fundamentales asociados a la seguridad de la información que son la integridad, la disponibilidad y la confidencialidad. Si bien el objetivo de la integridad garantiza que los datos permanezcan intactos e inalterables y disponibilidad por su lado que los mismo sean accesibles en cualquier momento, el objetivo de la confidencialidad es que esta información permanezca protegida y no se exponga sin el consentimiento de su titular.

Tal como lo describe García, 2016; "La confidencialidad, a veces denominada secreto o privacidad, es la condición, que asegura que la información no pueda estar disponible o ser descubierta por personas, entidades o procesos no autorizados" (Garc et al., 2016).

Cabe mencionar también que al ser un portal desarrollado e implementado hace tiempo atrás no contempla o cuenta con un estándar ISO (Organización Internacional de Normalización) como la ISO 27552. "Esta norma permite a las organizaciones implementar un Sistema de Gestión de Protección de Datos, con criterio equivalente y de complemento a un Sistema de Gestión de Seguridad de la Información, pero con énfasis en la protección de datos personal" (CALIDAR, 2019)

Sobre lo antes mencionado, el objetivo de esta ISO es permitir a las empresas implementar un SGPD (Sistema de Gestión de Protección de Datos) orientado a la protección de la privacidad en conjunto con las normas ISO 27001 e ISO 27002 y a su vez demuestren que están cumpliendo con la normativa en virtud del procesamiento de datos.

Conclusiones

La protección de datos de carácter personal genera un análisis de amenazas presentes como son: fraude comercial, espionaje, estafas, influir o influenciar a las personas, o aquellas que proveniente de la propia legislación que permite la exposición de información a través de la Ley Orgánica de Transparencia y Acceso a la Información Pública.

Para la sociedad actual estas amenazas generan preocupación tanto a nivel local e internacional, pues demuestran cómo se infringen los derechos humanos en cuanto a la privacidad y protección de datos se refiere, también revela la inseguridad de portales virtuales para el Registros de Datos Públicos; el insuficiente o nulo conocimiento sobre protección de los datos personales, y, la

necesidad de una Ley que contemple estos aspectos de manera íntegra y a su vez garantice los derechos fundamentales de los individuos.

En la actualidad atravesamos un momento histórico y a la vez crucial con respecto a los riesgos de la privacidad y protección de datos, en virtud de lo mencionado debemos tener presente que las políticas o normas que se instauren hoy para regular la información influirán sobre el tipo de sociedad que deseamos establecer y que se reflejara mañana. Como principales riesgos asociados a las tecnologías y la privacidad y protección de datos están los siguientes:

- Perder la información.
- Suplantación de identidad.
- Información en manos de desconocidos.
- Extorción, acoso, amenazas.
- Ser víctima de estafas (Phishing).
- Es más fácil de rastrear.
- Perdida de intimidad.

Recomendaciones

Teniendo en cuenta que, aunque en Ecuador la legislación contempla la Ley de protección de datos personales aún no existe conocimiento o un manejo adecuado de los mismos, sea por parte de las instituciones gubernamentales, las empresas o los mismos individuos, por lo que para proteger la información se puede recomendar lo siguiente:

- Utilizar contraseñas seguras, diferentes para cada cuenta.
- Utilizar navegadores alternativos para evitar rastreadores de datos.
- Evitar compartir información personal en redes sociales.
- Generar y mantener perfiles privados en plataformas digitales.
- Navegar solo por sitios seguros para evitar fraudes.
- Borrar historial y cache del navegador.
- Utilizar el cifrado de datos para proteger información.
- Recurrir a dispositivos externos para respaldar la información.
- Mantener actualizado el software para prevenir errores con fuga de datos.
- Considerar soluciones de seguridad como DLP (Data Loss Prevention).

- Registrarse en aplicaciones o servicios necesarios.
- Estar pendiente de comunicación/transmisión desatendida de cookies.
- Consentimiento de acceso a datos personales en dispositivos móviles.
- Segregar los servicios que compartan información.
- Revisar las políticas de uso.
- Limitar los datos que se suministra.
- Adoptar una posición proactiva.
- Investigar el uso que hacen las empresas sobre los datos personales.
- Conocer las normativas vigentes.
- Concientizar sobre la importancia de proteger los datos personales.
- Educarse y hacer conciencia en las personas.

Referencias

1. Arteaga, S. (2018). El escándalo de Cambridge Analytica afectó a 87 millones, dice Facebook. https://computerhoy.com/noticias/internet/escandalo-cambridge-analytica-afecto-87-millones-dice-facebook-78571
2. Barr, A., & Feigenbaum, E. A. (1981). The Handbook of Artificial Intelligence. sciencedirect. https://doi.org/https://doi.org/10.1016/C2013-0-07690-6
3. BBC News Mundo. (2019). Filtración de datos en Ecuador: la "grave falla informática" que expuso la información personal de casi toda la población del país sudamericano. BBC News. https://www.bbc.com/mundo/noticias-america-latina-49721456
4. CALIDAR. (2019). Nueva ISO 27552 – Gestión de Información Sobre Privacidad. https://calidar.pe/nueva-iso-27552-gestion-de-informacion-sobre-privacidad/
5. Cimpanu, C. (2019). Database leaks data on most of Ecuador's citizens, including 6.7 million children. https://www.zdnet.com/article/database-leaks-data-on-most-of-ecuadors-citizens-including-6-7-million-children/
6. Consejo para la Transparencia. (2013). Indice de Transparencia y Acceso a la Información. 1–64. http://www.consejotransparencia.cl/consejo/site/artic/20121213/asocfile/20121213160518/indice_de_transparencia_y_acceso_a_la_informaci__n.pdf

7. De, R. O. S., Del, H., Barrezueta, P., Organica, D. E. L. E. Y., La, D. E. G. D. E., & Datos, I. Y. (2016). Datos Civiles. 1–23.
8. Ecuador. (2019). Proyecto de ley organica de protección de datos (p. 52).
9. ESAN. (2019). El estado de la protección de datos personales en América Latina. https://www.esan.edu.pe/apuntes-empresariales/2019/04/el-estado-de-la-proteccion-de-datos-personales-en-america-latina/
10. Fedele, L., & Fedele, L. (2011). From Basic Maintenance to Advanced Maintenance. Methodologies and Techniques for Advanced Maintenance, 63–112. https://doi.org/10.1007/978-0-85729-103-5_5
11. Flores, C., Zambrano, D., Martínez, A., & Martínez, A. (2017). MANUAL DE USUARIO SISTEMA DE GESTIÓN DOCUMENTAL. 1, 96. http://www.funcionjudicial.gob.ec/www/pdf/MANUAL DE USUARIO SISTEMA DE GESTION DOCUMENTAL.pdf
12. Garc, G., Ledo, J. V., Inform, R., Consultante, P., Auxiliar, I., Nacional, E., & Clave, P. (2016). La informática y la seguridad. Un tema de importancia para el directivo. 3521, 47–58.
13. Giraldo, V. (2019). https://rockcontent.com/es/blog/plataformas-digitales/. Responsable Por La Estrategia de Internacionalización de Rock Content. https://rockcontent.com/es/blog/plataformas-digitales/
14. González, M. (2018). Qué ha pasado con Facebook: del caso Cambridge Analytica al resto de polémicas más recientes. https://www.xataka.com/legislacion-y-derechos/que-ha-pasado-con-facebook-del-caso-cambridge-analytica-al-resto-de-polemicas-mas-recientes
15. Izquierdo, R., Novillo, L., & Mocha, J. (2017). LAS REDES SOCIALES Y ADOLESCENCIAS. REPERCUSIÓN EN LA ACTIVIDAD FÍSICA. Universidad y Sociedad, 9(2), 313–318. https://orcid.org/0000-0003-0850-197X
16. Joel, E. G. (2001). Surgimiento de la sociedad de la información. Biblioteca Universitaria, 4, 77–86.
17. Judicatura, C. D. E. L. A. (2012). Consejo de la Judicatura: Experiencia mexicana. Boletín Mexicano de Derecho Comparado, 45(133), 375–387.

18. Monti, M., & Rasmussen, S. (2017). RAIN: A Bio-Inspired Communication and Data Storage Infrastructure. Artificial Life, 23(4), 552–557. https://doi.org/10.1162/ARTL_a_00247
19. Morales, A. A., & Karel Gomez Velázquez, Danisbel Rojas Rios, H. M. S. M. (2009). Sistema de autenticación , autorización y auditoría (AAA) para aplicaciones basadas en servicios Web XML Authentication , Authorization and Accounting (AAA) system to applications ba ... January 2009.
20. Moreno-Carriles, R. M. (2018). Big data; But what is it? Angiologia, 70(5), 191–194. https://doi.org/10.1016/j.angio.2018.05.001
21. Olivas Varela, J. A. (2011). Búsqueda eficaz de información en la Web. May, 126. http://www.researchgate.net/profile/Jose_Olivas/publication/228480257_Bsqueda_eficaz_de_informacin_en_la_Web/links/0c9605195fe85b5050000000.pdf
22. Oriza, J. (2018). Facebook y el escándalo con Cambridge Analytica. https://blogs.unitec.mx/vida-universitaria/facebook-y-el-escandalo-con-cambridge-analytica
23. Privacidad de datos en el mundo : Lo que realmente piensan los consumidores. (n.d.). 1–47.
24. Union Europea. (2018). Siete pasos. Comisión Europea.
25. Universidad de Costa Rica. Escuela de Historia, J. B., & Alpízar, L. M. A. (2010). Diálogos : revista electrónica de historia. Diálogos Revista Electrónica, 11(2), 71–88. https://revistas.ucr.ac.cr/index.php/dialogos/article/view/581/643
26. Winder, D. (2019). Personal Data Of Entire 16.6 Million Population Of Ecuador Leaked Online. https://www.forbes.com/sites/daveywinder/2019/09/16/personal-data-from-entire-166m-population-of-ecuador-leaked-online/?sh=7f07159c3705#326473943705