UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No. 023-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto
Guía para la aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura.
Línea de investigación
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento
Tecnologías de la Información y la Comunicación (TIC)
Autor
Evelyn Gabriela Arcos Rodríguez
Tutor
Mg. Renato Toasa PhD. Maryory Urdaneta

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Maryory Urdaneta con C.I.: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: Guía de aplicación para la protección de datos personales de personas intervinientes en procesos judiciales.

Elaborado por: Evelyn Gabriela Arcos Rodríguez, de C.I: 1722331061, estudiante de la Maestría en Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL**, como parte de los requisitos sustanciales con fines de obtener el Título de Magíster, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., 30 agosto del 2024

Firma

APROBACIÓN DEL TUTOR

Yo, Renato Toasa con C.I.: 1804724167, en mi calidad de Tutor del proyecto de investigación titulado: Guía de aplicación para la protección de datos personales de personas intervinientes en procesos judiciales.

Elaborado por: Evelyn Gabriela Arcos Rodríguez, de C.I: 1722331061, estudiante de la Maestría en Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magíster, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., 30 de agosto del 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Evelyn Gabriela Arcos Rodríguez con C.I: 1722331061, autora del proyecto de titulación denominado: Guía para la aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura. Previo a la obtención del título de Magíster en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.

3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., 30 de agosto del 2024.

EVELYN GABRIELA ARCOS RODRIGUEZ

Firmado digitalmente por EVELYN GABRIELA ARCOS RODRIGUEZ

Firma

Orcid: 0000-0003-2829-2351

Tabla de Contenido

Índice de figuras

Índice de Tabla

INFORMACIÓN GENERAL

Contextualización del tema

El Ecuador como un Estado constitucional de derechos y justicia garantiza una serie de derechos fundamentales individuales y colectivos como lo es por ejemplo el Derecho a la Información previsto en el artículo 18 de la Constitución de la República del Ecuador. Bajo este contexto, el 26 de mayo de 2021 entró en vigencia la Ley Orgánica de Protección de Datos Personales ante la necesidad de regular y proteger los datos personales tanto de los entes públicos como de los privados.

A medida que la sociedad ha avanzado, se han desarrollado herramientas legales y tecnológicas para regular el manejo de datos personales, tanto públicos como privados. No obstante, la recolección, almacenamiento, procesamiento, distribución o divulgación de estos datos requiere la autorización del titular o una disposición legal.

> "El uso de las telecomunicaciones posibilita la racionalización, la simplificación, la celeridad y el tratamiento de la información. De igual forma rompe las barreras clásicas del espacio y del tiempo. Ello supone indefectiblemente poder, facultades o posibilidades que han de ser reguladas, debido a que pueden ser lesivas de derechos y libertades fundamentales". (Rebollo, 2008).

La Ley Orgánica de Protección de Datos Personales ecuatoriana tiene una clara influencia de la normativa europea existente, por la efectividad que esta ha tenido en dicho continente, y lo que busca es proteger los derechos personales de los ciudadanos, por ello reconoce el derecho a la protección de datos como un derecho del ciudadano y no de las empresas. Además, establece como principio básico, la aplicación favorable al titular de los datos en caso de duda. (Asamblea Nacional, 2021).

> "Desde mediados de los años sesenta se constata en Europa la importancia del uso de las telecomunicaciones, así como la necesidad de una legislación que unifique pretensiones y especialmente que ofrezca un conjunto de medios de protección de los derechos y libertades fundamentales" (Rebollo, 2008).

El ámbito de aplicación de esta ley es para todas las entidades, tanto públicas como privadas, que tengan acceso al tratamiento de datos en el Estado ecuatoriano. Esto incluye datos personales que provengan de la oferta de bienes o servicios, así como los datos personales que provengan de contratos o regulaciones vigentes en el derecho internacional. (J. Casas Anguita, J.R. Repullo Labrador y J. Donado Campos, 2002).

El objetivo central de la ley es mejorar la seguridad de la información en cuanto a los datos personales de las organizaciones y personas que trabajen en ellas, salvaguardar la base de datos que manejan las entidades con referencia a sus clientes y regular la confidencialidad de los datos personales para evitar que se usen con otros fines.

Bajo este contexto, la vigencia de esta ley ha permitido que el Consejo de la Judicatura expida el Reglamento para el tratamiento de Datos Personales dentro de Procesos Judiciales, cuya finalidad consiste en proteger los derechos al honor, buen nombre, datos personales y no discriminación por pasado judicial de los sujetos intervinientes en procesos judiciales.

Problema de la investigación

Cuando una persona es sujeto procesal, sobre todo, dentro de un procedimiento de orden penal que implica el presunto cometimiento de un delito, los sujetos intervinientes que son objeto de imputación de la infracción penal llegan a ser discriminados por el simple hecho de verse incursos en un proceso de tal naturaleza, sin considerar que constitucionalmente todas las personas gozan de presunción de inocencia, de modo que estos son inocentes hasta que se demuestre lo contrario.

> "**Constitución de la República:** Art. 76.- En todo proceso en el que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso que incluirá las siguientes garantías básicas: 2. Se presumirá la inocencia de toda persona, y será tratada como tal, mientras no se declare su responsabilidad mediante resolución firme o sentencia ejecutoriada."

El Artículo 76 de la Constitución de la República es fundamental en el problema planteado porque establece el derecho al debido proceso y la presunción de inocencia, que son esenciales para proteger los derechos de las personas implicadas en procesos penales, este artículo cobra relevancia por varias razones:

a.- ***Presunción de Inocencia:*** El inciso 2 del Artículo 76 establece que toda persona es presumida inocente y debe ser tratada como tal hasta que se declare su responsabilidad mediante una resolución firme o sentencia ejecutoriada. Esto significa que cualquier individuo sujeto a un proceso penal debe ser considerado inocente mientras no se demuestre lo contrario de manera definitiva.

b.- ***Prevención de Discriminación:*** La discriminación de personas involucradas en procesos penales, como se menciona en el problema de la investigación, viola el principio de presunción de inocencia. Tratar a alguien como culpable antes de una sentencia firme es contrario a los derechos garantizados por la Constitución y puede llevar a estigmatización y trato injusto.

c.- ***Derecho al Debido Proceso:*** El debido proceso asegura que todas las etapas del procedimiento legal se realicen de manera justa y equitativa. Incluye el derecho a un juicio justo, la posibilidad de defensa adecuada, y otras garantías procesales que protegen los derechos de los acusados.

d.- ***Protección de Datos Personales:*** En el marco de la Ley de Protección de Datos, es crucial que la información personal de los sujetos procesales sea manejada con cuidado y confidencialidad, especialmente cuando se trata de personas que aún no han sido condenadas. Publicar o manejar indebidamente esta información puede vulnerar su derecho a la presunción de inocencia y al debido proceso.

e.- ***Relevancia Constitucional:*** Utilizar el Artículo 76 como fundamento en la guía para la aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura subraya la importancia de respetar los derechos constitucionales de los individuos en todo momento, especialmente en situaciones de procedimientos penales donde la reputación y los derechos de las personas pueden verse seriamente afectados.

> "**Código Orgánico Integral Penal:** Art. 605.- Sobreseimiento. - La o el juzgador dictará auto de sobreseimiento en los siguientes casos: 1. Cuando la o el fiscal se abstenga de acusar y de ser el caso, dicha decisión sea ratificada por el superior. 2. Cuando concluya que los hechos no constituyen delito o que los elementos en los que la o el fiscal ha sustentado su acusación no son suficientes para presumir la existencia del delito o participación de la persona procesada. 3. Cuando encuentre que se han establecido causas de exclusión de la antijuridicidad".

Bajo este contexto, la Función Judicial cuenta con el denominado Sistema Automático de Trámite Judicial Ecuatoriano (SATJE) mediante el cual se registran todo tipo de actuaciones judiciales de diverso orden, siendo este un sistema que contiene información de acceso público, es decir, que cualquier persona puede obtener información de si un sujeto ha enfrentado un proceso penal o no, de si ha sido sobreseído o de si ha sido condenado o se ha ratificado su inocencia.

En tal virtud, para aquellas personas que han debido afrontar por motivo de cualquier orden un proceso penal pero que han sido objeto de sobreseimiento o sentencia ratificatoria de inocencia es indispensable poder proteger sus datos con la finalidad de precautelar sus derechos al honor y al buen nombre, pues como se dijo anteriormente, son un problema los prejuicios que la sociedad en general expone en contra de estos sujetos procesales.

Objetivo General

- Elaborar una guía de aplicación para la protección de datos personales de personas intervinientes en procesos judiciales.

Objetivos Específicos

- Contextualizar los fundamentos teóricos básicos sobre el tratamiento de datos personales de conformidad con la Ley Orgánica de Protección de Datos Personales.
- Diagnosticar la situación actualidad del consejo de la judicatura referente a la ley de protección de datos.
- Diseñar la guía para la solicitud de protección de datos personales de las personas intervinientes en procesos judiciales de naturaleza penal que han sido sobreseídos o han obtenido sentencias ratificatorias de inocencia.
- Validar la guía mediante el criterio de especialistas jurídicos en materia constitucional y legal.

Vinculación con la sociedad y beneficiarios directos

El principal beneficiario de la guía de aplicación para la protección de datos personales de personas intervinientes en procesos judiciales en este caso en particular es la sociedad en general y específicamente aquellas personas que han atravesado procesos penales y que han obtenido autos de sobreseimiento o sentencias ratificatorias de inocencia.

Recientemente, el 26 de febrero de 2024 el Pleno del Consejo de la Judicatura expidió la Resolución No. 043-2024 que contiene el Reglamento para el Tratamiento de Datos Personales dentro de Procesos Judiciales, describiendo de manera muy sucinta la posibilidad de modificar, rectificar u ocultar datos personales de aquellos sujetos que han intervenido en procesos judiciales en general, cuya fuente legal es, además de la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales.

La Ley Orgánica de Protección de Datos trae consigo numerosos beneficios para la sociedad, pues se ha implementado con el propósito de salvaguardar la privacidad de los ciudadanos y fortalecer la seguridad en el manejo de la información personal tanto de las personas jurídicas como de las personas naturales.

En este sentido, todas las instituciones tanto públicas como privadas deben obtener el consentimiento expreso de las personas antes de utilizar sus datos, para de esta forma garantizar que los ciudadanos tengan un mayor control sobre su información personal, creando de esta forma un ambiente más seguro; disuadiendo a las empresas y organizaciones de realizar prácticas ilegales o irresponsables en el manejo de la información personal por las sanciones severas de la mal utilización de información.

En resumen, la nueva ley de protección de datos de Ecuador beneficia a la sociedad, al salvaguardar la privacidad de los ciudadanos, fortalecer la seguridad en el manejo de la información personal, fomentar la transparencia y promover una mayor profesionalización en este ámbito. Es un paso importante hacia la protección de los derechos digitales de los ciudadanos y ayuda a construir una sociedad más segura y confiable en el uso de las tecnologías de la información.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1 Contextualización general del estado del arte

La protección de datos personales es una figura jurídica que refiere las medidas y regulaciones que se deben considerar para garantizar la seguridad y privacidad de la información personal de las personas, salvaguardando el derecho de los individuos al buen nombre y al honor. La protección de estos derechos es de orden constitucional, pues la Constitución de la República del Ecuador garantiza a través de la ley, la protección de la imagen y voz de una persona, lo cual guarda armonía con el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión de uso de la información y datos personales, así como su correspondiente protección. (Asamblea Nacional, 2021).

En este sentido, cuando una persona es titular de datos personales constantes en una base de datos, es esta persona quien se encuentra en la capacidad de autorizar el uso de los mismos, así como su rectificación, eliminación o anulación tomando en cuenta que también se debe respetar el principio de publicidad de la información, específicamente cuando nos referimos a información constante en la base de datos de procesos judiciales al cual se puede acceder a través del Sistema Ecuatoriano de Trámite Judicial Ecuatoriano. (J. Casas Anguita, J.R. Repullo Labrador y J. Donado Campos, 2002)

1.1.1 Introducción al contexto legal y tecnológico:

La judicatura es un entorno en el que la gestión de datos juega un papel esencial. En el ámbito legal, la información personal y confidencial de individuos y casos legales se recopila, almacena y utiliza de manera rutinaria. La Ley de Protección de Datos se convierte en un elemento crucial en este contexto para garantizar la privacidad y la seguridad de los datos en el sistema judicial.

La ley puede requerir que las autoridades judiciales notifiquen a las partes afectadas en caso de una violación de datos, lo que garantiza la transparencia y la oportunidad en la divulgación de incidentes de seguridad. La gestión de historiales legales y registros es fundamental en la judicatura. La ley garantiza que los individuos tengan derechos sobre su información legal y personal, como el acceso a sus registros y el derecho a solicitar correcciones. (ELLIE KEEN, 2016)

Además, establece las pautas para compartir información entre las partes involucradas en procesos legales, como litigantes, testigos y peritos, asegurando que se respeten los derechos de privacidad y confidencialidad. La correcta aplicación de la Ley de Protección de Datos en el sector judicial es fundamental para mantener la confianza en el sistema legal y garantizar que los datos personales y confidenciales estén debidamente protegidos. Esta legislación también puede tener implicaciones significativas en la gestión de casos legales, especialmente en lo que

respecta a la evidencia digital y la presentación de pruebas electrónicas. (Asamblea Nacional, 2021).

La Ley de Protección de Datos, también conocida como normativas de privacidad o leyes de privacidad de datos, tiene sus raíces en la preocupación por la reserva y la protección de la información particular. A lo largo del tiempo, varios eventos y desarrollos contribuyeron al establecimiento de estas leyes. Aquí hay algunos hitos importantes en el desarrollo de la protección de datos:

- ***Declaración Universal de Derechos Humanos de 1948:*** Estableció el derecho a la privacidad como un derecho fundamental. El Art. 12 de la Declaración sostiene que "Nadie será objeto de injerencias arbitrarias en su vida privada" (Ley de protección, 2021).

- ***Prácticas Justas de Información (década de 1970):*** Estas prácticas, también conocidas como principios de privacidad, establecieron pautas para la recopilación y uso de datos personales, incluyendo notificación, elección, acceso y seguridad (Ley de protección, 2021).

- ***Directiva 95/46/CE de la Unión Europea (1995):*** Sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta directiva sentó las bases para las leyes de privacidad en los Estados miembros de la UE (Encuesta, 2020).

- ***Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA) de EE. UU. (1996):*** Estableció normas para la protección de la información de salud.

- ***Ley de Puerto Seguro (Safe Harbor):*** Este acuerdo entre EE. UU. y la UE permitía la transmisión de datos personales entre organizaciones empresariales de la UE y organizaciones de EE. UU. que cumplieran con ciertos principios de privacidad. Sin embargo, fue invalidado por el Tribunal de Justicia de la Unión Europea en 2015.

- ***Reglamento General de Protección de Datos (GDPR) de la UE (2018):*** Reemplazó la Directiva de Protección de Datos de la UE y estableció estándares más estrictos y uniformes para la protección de datos en todos los estados miembros de la UE. Introdujo sanciones significativas por violaciones de privacidad y otorgó a los individuos un mayor control sobre sus datos personales.

Estos eventos y regulaciones han influido en el desarrollo de leyes de protección de datos en todo el mundo. Muchos países han adoptado o adaptado sus propias normativas para abordar las preocupaciones sobre la privacidad en la era digital.

En el Ecuador, se ha tenido un avance significativo que ha llevado tiempo. Después de casi 19 años, se aprobó la legislación de protección de datos en Ecuador (LOPDP). La Ley Orgánica de Protección de Datos Personales (LOPDP) fue la primera ley en Ecuador que abordó específicamente la protección de datos personales. Se establecieron principios y obligaciones para el tratamiento de datos personales, así como los derechos de los titulares de datos. También se creó la Agencia de Regulación y Control de Datos Personales (ARCO) para supervisar y asegurar que se respeten las normas legales establecidas. La ARCO tiene la responsabilidad de recibir quejas, realizar investigaciones y aplicar sanciones en casos de violaciones a la privacidad.

Las leyes de protección de datos suelen evolucionar para adaptarse a los cambios tecnológicos y a las nuevas prácticas en el tratamiento de la información. La armonización con normativas internacionales también es un factor importante. Por ejemplo, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea ha influido en muchas legislaciones en todo el mundo, y algunos países pueden considerar alinearse con estos estándares internacionales.

Es importante estar atento a los acontecimientos recientes en el ámbito legal y de privacidad en Ecuador para obtener información actualizada sobre cualquier cambio en la legislación de protección de datos.

1.1.2 Principios sobre la Privacidad y la Protección de Datos Personales:

La protección de datos personales es un tema crucial en la era digital, donde la privacidad enfrenta desafíos constantes derivados del avance tecnológico y la globalización de la información. En este contexto, la Organización de los Estados Americanos (OEA), a través de su Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos, ha desarrollado una serie de Principios Actualizados sobre la Privacidad y la Protección de Datos Personales.

Este marco normativo busca armonizar las legislaciones nacionales en el ámbito del continente americano, promoviendo un enfoque uniforme y coherente que respete los derechos fundamentales de los individuos y garantice una protección efectiva de sus datos personales.

Los principios actualizados abordan aspectos fundamentales como el consentimiento informado, el manejo y tratamiento justo de los datos, la transparencia en su uso, y medidas de seguridad robustas para prevenir accesos no autorizados o malintencionados. También se enfatizan la importancia de la portabilidad de los datos, el derecho a la rectificación y la cancelación de datos, y el tratamiento de datos sensibles con especial cuidado.

Este documento se posiciona como una herramienta esencial para legisladores, empresas, organizaciones y ciudadanos interesados en la defensa de la privacidad y la integridad de la información personal. A través de estos principios, la OEA busca fortalecer la confianza en el manejo de datos personales y fomentar una cultura de privacidad. (Principios actualizados sobre la privacidad y la proteccion de datos personales, 2019).

Principio 1 - Finalidades Legítimas y Lealtad

Los datos personales deben ser recolectados únicamente para propósitos legítimos y utilizando métodos que sean justos y apropiados.

Principio 2 - Transparencia y Consentimiento

Al momento de recopilar los datos, se debe identificar claramente quién es el responsable de ellos, especificar para qué fines serán utilizados, cuál es la base legal para su tratamiento, y quiénes recibirán estos datos. Además, es importante que se informe a las personas sobre sus derechos con respecto a sus datos. Si el tratamiento se basa en el consentimiento, éste debe ser previo, claro, libre e informado.

Principio 3 - Pertinencia y Necesidad

Solo deben recopilarse aquellos datos personales que sean adecuados, pertinentes y estrictamente necesarios para cumplir con los fines específicos para los cuales se recolectan y procesan.

Principio 4 - Tratamiento y Conservación Limitados

El procesamiento y almacenamiento de datos personales deben realizarse únicamente de manera legítima y compatible con los fines originales de su recolección. Su retención no debe extenderse más allá del tiempo necesario para cumplir con dichos propósitos, conforme a la legislación vigente.

Principio 5 – Confidencialidad

Los datos personales no deben divulgarse ni compartirse con terceros, ni usarse para fines distintos de aquellos para los que fueron recolectados, salvo que se obtenga el consentimiento de la persona involucrada o exista una disposición legal que lo permita.

Principio 6 - Seguridad de los Datos

La protección de la confidencialidad, integridad y disponibilidad de los datos personales debe garantizarse mediante medidas de seguridad adecuadas, tanto técnicas como organizativas, para prevenir accesos no autorizados, pérdidas, destrucción, daños o divulgaciones, incluso si ocurren accidentalmente. Estas medidas deben ser auditadas y actualizadas regularmente.

Principio 7 - Exactitud de los Datos

Es crucial mantener los datos personales precisos, completos y actualizados en la medida necesaria para cumplir con los fines de su procesamiento, evitando que se distorsione su veracidad.

Principio 8 - Acceso, Rectificación, Cancelación, Oposición y Portabilidad

Se deben establecer mecanismos sencillos, efectivos y accesibles para que las personas puedan solicitar acceso, rectificación o eliminación de sus datos personales, así como oponerse a su procesamiento y, cuando sea aplicable, ejercer su derecho a la portabilidad de dichos datos. Generalmente, estos derechos deben ser gratuitos. Si es necesario restringir alguno de estos derechos, dicha limitación debe estar claramente especificada en la legislación nacional y cumplir con los estándares internacionales pertinentes.

Principio 9 - Datos Personales Sensibles

Algunos datos personales, debido a su naturaleza sensible en ciertos contextos, tienen un mayor potencial de causar daño si se manejan incorrectamente. Las categorías de estos datos y su nivel de protección deben ser claramente establecidos en la legislación y regulaciones nacionales. Los responsables de estos datos deben implementar medidas de privacidad y seguridad adecuadas al grado de sensibilidad y al posible daño que podrían causar.

Principio 10 – Responsabilidad

Quienes gestionen y procesen datos personales deben adoptar e implementar medidas técnicas y organizativas adecuadas para garantizar y demostrar que el tratamiento se realiza en conformidad con estos Principios. Dichas medidas deben ser auditadas y actualizadas de manera regular. Además, deben cooperar con las autoridades de protección de datos personales cuando sea requerido.

Principio 11 - Flujo Transfronterizo de Datos y Responsabilidad

Reconociendo la importancia del flujo de datos personales para el desarrollo económico y social, los Estados Miembros deben colaborar para facilitar el intercambio de datos personales entre países que ofrezcan un nivel de protección adecuado, conforme a estos Principios. También deben trabajar en la creación de mecanismos y procedimientos que aseguren que las entidades responsables del tratamiento de datos en más de una jurisdicción cumplan con estos Principios.

Principio 12 – Excepciones

Cualquier excepción a estos Principios debe estar explícitamente prevista en la legislación nacional, ser comunicada al público y limitarse a razones de soberanía nacional, seguridad nacional, seguridad pública, salud pública, combate a la criminalidad, cumplimiento de normativas u otros intereses públicos.

Principio 13 - Autoridades de Protección de Datos

Los Estados Miembros deben establecer órganos de supervisión independientes, con los recursos necesarios, que estén alineados con la estructura constitucional y administrativa de cada Estado, para monitorear y promover la protección de datos personales de acuerdo con estos Principios. Además, se debe fomentar la cooperación entre dichos órganos.

1.1.2 Derechos digitales

En la actualidad el uso de internet se ha vuelto indispensable para la vida cotidiana, la protección y promoción de los derechos humanos en el ámbito digital es más crítica que nunca. Reconociendo esta necesidad, el Consejo de Europa ha elaborado la "Guía de los Derechos Humanos para los Usuarios de Internet", bajo la Recomendación CM/Rec(2014)6. Este documento esencial proporciona una orientación clara sobre cómo los derechos humanos establecidos a nivel internacional se aplican en el contexto digital, asegurando que los usuarios de internet puedan ejercer sus derechos de manera plena y efectiva mientras navegan en línea. (ELLIE KEEN, 2016).

a. Acceso y no discriminación

1. Acceso a Internet: Deberías tener acceso continuo a Internet, siendo la desconexión una medida excepcional, solo justificada por decisión judicial o condiciones contractuales extremas.
2. Asequibilidad y no discriminación: El acceso a Internet debería ser económicamente accesible y sin discriminación, permitiéndote acceder a contenido, aplicaciones y servicios libremente.
3. Soporte a grupos vulnerables: Si perteneces a un grupo vulnerable (zona rural, bajos ingresos, discapacidades), las autoridades deben esforzarse por facilitar tu acceso a Internet.
4. No discriminación en servicios: No debes enfrentar discriminación por parte de proveedores de servicios o autoridades en Internet basada en género, raza, edad, orientación sexual, entre otros.

b. Libertad de expresión e información

1. Libertad de expresión: Tienes derecho a expresarte libremente en línea y acceder a diversas opiniones y expresiones, incluso aquellas que puedan ser controversiales.
2. Restricciones a la libertad de expresión: Cualquier restricción a la libertad de expresión debe ser legal, precisa y supervisada judicialmente, especialmente si incita a la discriminación, odio o violencia.
3. Derechos de autor: Debes respetar los derechos de propiedad intelectual al crear y distribuir contenido.
4. Protección de la libertad de expresión: Las autoridades deben salvaguardar tu derecho a expresar tus opiniones y de información, asegurando que las restricciones sean legítimas y proporcionales.
5. Responsabilidad de proveedores de servicios: Los proveedores de servicios online deben venerar tus derechos humanos y ofrecerte mecanismos para gestionar demandas.

c. Reunión, asociación y participación

1. Libertad de reunión en línea: Puedes utilizar Internet para formar o unirte a grupos y asociaciones sin restricciones formales por parte de autoridades.
2. Protesta en línea: Tienes derecho a protestar en línea, siempre y cuando no infrinjas la ley o cause daños a terceros.
3. Participación en procesos democráticos: Puedes usar herramientas online para participar en debates políticos y procesos legislativos.

d. Protección de la vida privada y de los datos personales

1. Privacidad y datos personales: Debes ser consciente de que tus datos personales son constantemente procesados online y tienes derecho a controlar este proceso.
2. Tratamiento de datos: El manejo de tus datos personales debe realizarse de manera legal y con tu consentimiento, brindando información clara sobre cómo serán utilizados.
3. Interceptaciones y vigilancia: No debes ser objeto de vigilancia generalizada y cualquier quebrantamiento de tu privacidad debe estar claramente justificado y regulado.
4. Privacidad en el trabajo: Tu vida privada y comunicaciones deben ser respetadas en el trabajo, con políticas claras sobre cualquier vigilancia.

e. Educación y conocimientos básicos

1. Acceso a la educación online: Deberías tener acceso a educación y recursos culturales y académicos en línea, respetando los derechos de autor.
2. Conocimientos digitales: Debes tener acceso a educación que te permita entender y utilizar herramientas digitales críticamente.

f. Niños y jóvenes

1. Participación de menores: Como joven, tienes derecho a expresarte y participar en la sociedad, con tus opiniones consideradas de acuerdo a tu edad y madurez.
2. Orientación sobre uso seguro de Internet: Debes recibir información y orientación apropiada sobre cómo navegar de forma segura en Internet.
3. Protección contra contenidos dañinos: Siempre tienes el derecho a solicitar la eliminación de contenido perjudicial relacionado contigo en Internet.
4. Protección contra ciberdelincuencia: Debes recibir protección especial contra abusos en Internet y tener acceso a recursos para denunciar comportamientos ilegales en línea.
5. Tienes derecho a recibir protección especial que garantice tu bienestar físico, mental y moral, incluyendo medidas específicas contra el abuso, la explotación sexual en línea y otras formas de ciberdelincuencia.

g. Recursos efectivos

1. Cuando tus derechos humanos y libertades fundamentales se vean restringidos o violados, tienes derecho a un recurso efectivo sin necesidad de iniciar una acción legal. Los recursos deben ser conocidos, accesibles, asequibles y capaces de ofrecer una reparación adecuada.
2. Estos recursos pueden incluir investigación, explicación, corrección, y compensación, y deben poder obtenerse de proveedores de servicios de Internet, autoridades gubernamentales o instituciones nacionales dedicadas a la protección de derechos humanos.

h. Información y Orientación

1. Los proveedores de servicios y autoridades deben informarte sobre tus derechos y los recursos disponibles, y proporcionarte medios para denunciar violaciones y buscar reparación.
2. Instituciones como autoridades de protección de datos y oficinas de asesoramiento deben ofrecer información adicional y orientación sobre cómo proteger tus derechos.

3. Las autoridades nacionales deben protegerte de actividades ilegales en Internet, investigar delitos y tomar medidas si se viola tu identidad digital o propiedad en línea.

Derecho a un Proceso Justo

Tienes derecho a un juicio justo y a ser juzgado en un período razonable por un tribunal que actúe de manera objetiva e imparcial. Si tus derechos han sido violados, puedes recurrir al Tribunal Europeo de Derechos Humanos después de haber agotado todos los medios legales nacionales (Consejo de Europa, 2014).

1.1.4 Trabajos Relacionados

El derecho a la privacidad fue inicialmente reconocido en la Declaración Universal de Derechos Humanos de 1944. Alemania fue precursora en la protección de datos, con la primera ley europea sobre el tema en 1970, seguida por la Privacy Act de Estados Unidos en 1974. En España, este derecho se establece en el artículo 18.1 de la Constitución, que asegura la intimidad personal y familiar y la propia imagen. Posteriormente, en 1992, se promulgó la Ley Orgánica 5/92 (LORTAD), en cumplimiento del mandato del artículo 18.4 de la Constitución, que busca limitar el uso de la informática para proteger la intimidad personal. La LORTAD fue desarrollada más adelante mediante varios reales decretos. En 1995, la Unión Europea aprobó la Directiva 95/46/CE, que establece requisitos mínimos para el tratamiento de datos personales, seguida por la Ley Orgánica 15/1999 (LOPD) en España, que adaptaba la ley española a la directiva y mejoraba aspectos de la LORTAD. Más tarde, en 2007, se promulgó el Reglamento de desarrollo de la LOPD para abordar los riesgos del manejo de datos personales. Finalmente, el Reglamento General de Protección de Datos (RGPD) de la UE, introducido en 2016 y plenamente aplicable en 2018, actualiza y sustituye la Directiva 95/46/CE, estableciendo un marco jurídico uniforme para todos los estados miembros con aplicación directa y requisitos mínimos de adaptación nacional, reflejando los avances tecnológicos y la necesidad de una normativa homogénea en el manejo de datos personales (Pérez Rodríguez, M. D. (Coord.), 2017).

En investigaciones previas relacionadas con la protección de datos personales, se ha evidenciado la importancia de contar con un marco normativo claro y específico para garantizar la efectividad de la Ley de Protección de Datos.

Por ejemplo, en el estudio realizado por Hernández Alvarado et al. (2023), se destaca la carencia de un reglamento complementario para la Ley Orgánica de Protección de Datos en Ecuador, lo que ha generado dificultades en la correcta aplicación y protección de los datos personales de los ciudadanos ecuatorianos. Asimismo, se ha señalado la necesidad de establecer

pautas claras y específicas para el tratamiento de datos personales, especialmente en entornos judiciales, donde la sensibilidad y confidencialidad de la información son fundamentales.

En este sentido, la presente tesis se enmarca en la línea de investigación que busca desarrollar una guía para la aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura, con el objetivo de brindar orientación y herramientas prácticas para garantizar el cumplimiento normativo y la protección efectiva de los datos personales en el ámbito judicial. A través de un enfoque metodológico mixto, se pretende explorar las implicaciones de la ausencia de un reglamento específico en la aplicación de la ley, identificar buenas prácticas y recomendaciones para el tratamiento de datos sensibles en el contexto judicial, y contribuir al fortalecimiento de la cultura de protección de datos en el Consejo de la Judicatura y en el sistema judicial ecuatoriano en su conjunto.

En el contexto de la protección de datos en entidades judiciales, se han realizado diversos estudios y análisis que abordan la importancia de garantizar la privacidad y seguridad de la información en el ámbito judicial. Por ejemplo, Miralles (2010). Destaca la relevancia del derecho a la protección de datos como un mecanismo fundamental para preservar la autodeterminación informativa de los individuos y garantizar un control efectivo sobre sus datos personales.

Asimismo, se ha señalado la necesidad de establecer directrices claras y procedimientos específicos para el tratamiento de datos en instituciones judiciales, como se aborda en el artículo de referencia.

Además, la normativa vigente, como la Ley Orgánica de Protección de Datos (LOPD), establece requisitos y obligaciones específicas para el tratamiento de datos personales en el ámbito judicial, lo cual resalta la importancia de contar con guías y protocolos adaptados a las particularidades de este sector. En este sentido, la investigación proporciona un marco de referencia para la implementación de medidas de protección de datos en el Consejo de la Judicatura, abordando aspectos clave como la notificación de transferencias internacionales, el consentimiento del afectado y las garantías de respeto a la privacidad en los procesos judiciales.

En resumen, la aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura requiere de una aproximación integral que considere tanto los principios legales como las particularidades operativas de la institución, con el objetivo de asegurar el cumplimiento normativo y la salvaguarda de los derechos fundamentales de los ciudadanos en el ámbito judicial.

1.2 Proceso investigativo metodológico

La presente investigación se estructura bajo un enfoque cuantitativo, complementado por métodos exploratorios y explicativos. La naturaleza cuantitativa de este estudio permite una análisis sistemático y objetivo de los datos recogidos a través de encuestas aplicadas a los servidores del CJ de la Planta Matriz.

Este enfoque se enriquece mediante un marco teórico robusto que incluye una profunda revisión de literatura jurídica y aportes de profesionales con amplia experiencia en derecho administrativo, lo que facilita la evaluación de las percepciones y opiniones en el ámbito jurídico (Pérez de Tudela, 2014). Adicionalmente, el estudio adopta niveles exploratorios y explicativos para analizar desde un principio general a conclusiones más detalladas, particularmente en temas relacionados con la nueva Ley de Protección de Datos Personales y su impacto en los servidores públicos (Juan Báez y Pérez de Tudela, 2014).

1.2.1 Instrumentos y técnicas de investigación:

Los instrumentos utilizados en esta investigación incluyen principalmente encuestas estructuradas que se aplicaron a los servidores públicos del CJ de la Planta Matriz. Estas encuestas fueron diseñadas para capturar datos cuantitativos sobre actitudes, creencias y opiniones respecto a la normativa y prácticas jurídicas. Adicionalmente, se ha realizado una revisión exhaustiva de fuentes secundarias, incluyendo literatura jurídica, normativa vigente y estudios previos, para complementar y corroborar los datos obtenidos. La combinación de estos métodos facilita una comprensión integral y multifacética de los temas investigados, permitiendo tanto la identificación de tendencias generales como el análisis en profundidad de aspectos específicos relacionados con el marco legal actual y su percepción entre los profesionales del derecho. (J. Casas Anguita, J.R. Repullo Labrador y J. Donado Campos, 2002).

Es esencial contar con una encuesta bien estructurada que recopile datos precisos y relevantes.

Por ello, se propone un modelo de encuesta para servidores públicos, especialmente diseñada para evaluar la percepción, el conocimiento y las prácticas actuales en relación con la protección de datos personales en el ámbito judicial TIC, el objetivo es recoger información para desarrollar una guía práctica que mejore la gestión de la protección de datos personales en procesos judiciales, en el contexto de las TIC.

1.2.2 Criterios éticos y legales:

Esta investigación se ha adherido estrictamente a los principios éticos y legales necesarios para la investigación socio-jurídica. Se ha garantizado la confidencialidad y el anonimato de todos los participantes en la encuesta, asegurando que toda la información recopilada se maneje con el mayor grado de privacidad y respeto por los derechos de los informantes. Además, se ha obtenido la aprobación informado de todos los colaboradores, clarificando el propósito de la investigación, los usos de los datos recopilados y la voluntariedad de su cooperación. Desde el punto de vista legal, el estudio se ha desarrollado conforme a la normativa vigente sobre protección de datos personales, en línea con la Ley Orgánica de Protección de Datos Personales, asegurando así el cumplimiento de todos los requisitos legales pertinentes y contribuyendo a la integridad y validez de la investigación.

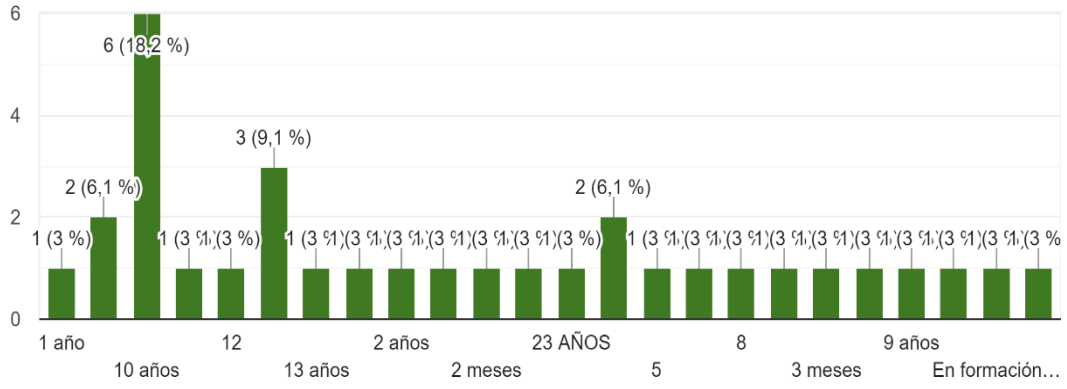
Estos elementos metodológicos y éticos aseguran la rigurosidad del estudio y la relevancia de sus contribuciones al ámbito del derecho administrativo y la protección de datos personales, facilitando así su aplicabilidad y utilidad para la mejora de políticas y prácticas en el sector público.

En el anexo 3 se detalla la encuesta realizada

1.3 Análisis de resultados

Figura 1

Distribución de la Experiencia laboral en el sistema judicial

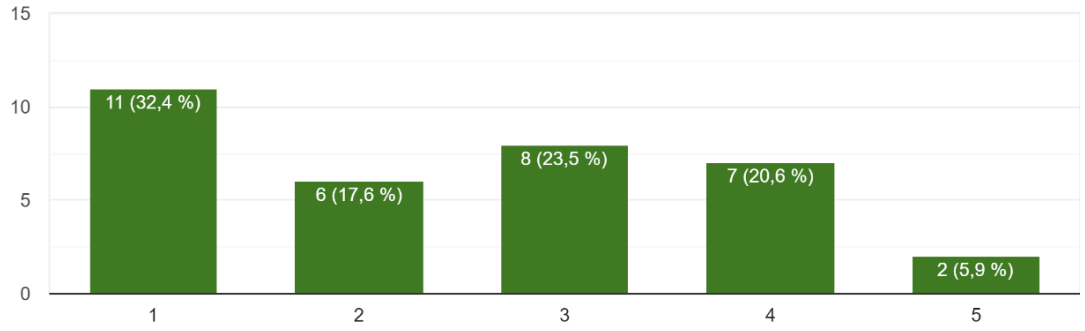


Nota. La figura muestra la proporción de encuestados según el número de años de experiencia en el sistema judicial.

Análisis: La distribución de la experiencia laboral en el sistema judicial revela una mezcla significativa entre la nueva incorporación y la experiencia consolidada. El 18.2% de los encuestados tienen solo 1 año de experiencia, lo que podría indicar una alta rotación o una reciente expansión en el personal, mientras que un 15.2% adicional tiene 3 años, sugiriendo un grupo intermedio con algo más de familiaridad con el entorno judicial. Un porcentaje similar está en formación, lo que podría reflejar la integración de nuevos talentos en el sistema. Los restantes encuestados tienen experiencia que varía desde 2 hasta 23 años, aunque en menor proporción. Esta diversidad en la experiencia indica un rango amplio de conocimientos y habilidades dentro del Consejo de la Judicatura, lo que puede influir en la percepción y aplicación de la Ley de Protección de Datos, destacando la necesidad de enfoques de formación y políticas adaptadas a los diferentes niveles de experiencia.

Figura 2

Evaluación de la formación específica en protección de datos personales

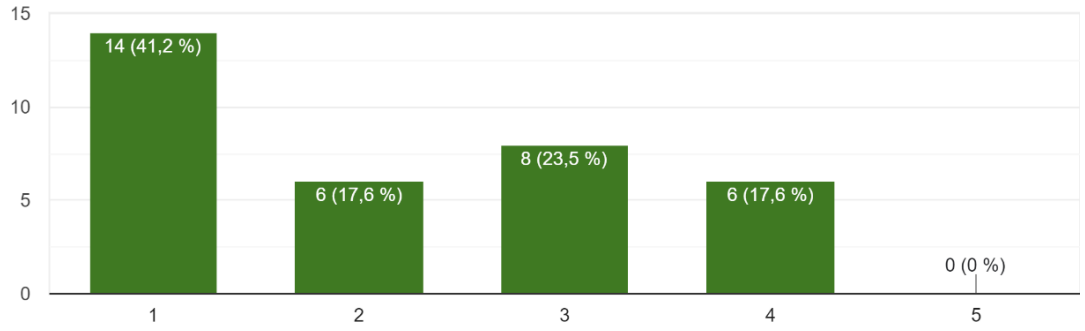


Nota. Esta figura ilustra el grado de acuerdo de los encuestados con la afirmación de haber recibido una formación específica en protección de datos personales.

Análisis: La evaluación sobre la formación específica en protección de datos personales muestra una percepción bastante diversa entre los encuestados. Un 32.4% de los participantes está en total desacuerdo con haber recibido una formación adecuada, lo que indica una insatisfacción notable. Un 17.6% también está en desacuerdo, aunque en menor grado. El 23.5% se encuentra en una posición neutral, sugiriendo que la formación podría no haber sido completamente satisfactoria ni insuficiente. En contraste, el 20.6% está de acuerdo con haber recibido una formación adecuada, y solo el 5.9% está en total acuerdo con ello. Esta variabilidad en las respuestas sugiere que, en general, la formación en protección de datos no es percibida de manera uniforme entre los empleados, indicando una necesidad de mejorar la calidad.

Figura 3

Percepción sobre la Suficiencia de la Formación en Protección de Datos Personales

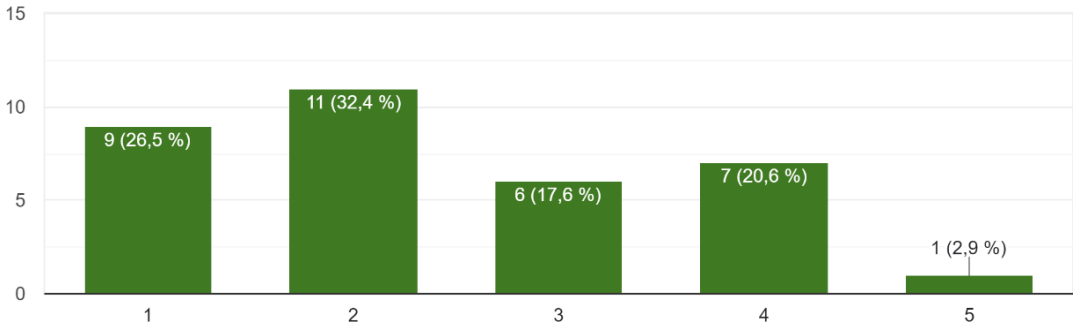


Nota. La figura representa la percepción de los encuestados sobre si la formación en protección de datos personales es suficiente.

Análisis: La percepción de la suficiencia de la formación en protección de datos personales revela una insatisfacción predominante. Un 41.2% de los encuestados está completamente en desacuerdo con la afirmación de que la formación recibida es suficiente, lo que indica una fuerte insatisfacción con el contenido o la extensión de la formación. Un 17.6% adicional está en desacuerdo, reflejando una percepción similar, aunque en menor grado. El 23.5% se encuentra en una posición neutral, lo que puede indicar que algunos participantes no tienen una opinión definida sobre la suficiencia de la formación. Por otro lado, un 17.6% está de acuerdo con la afirmación, mientras que ninguno de los encuestados considera que la formación recibida es completamente suficiente. Este patrón destaca una necesidad clara de mejorar la formación en protección de datos para que sea percibida como adecuada por una mayor proporción de los empleados.

Figura 4

Familiaridad con las Políticas de Protección de Datos Personales en el Juzgado

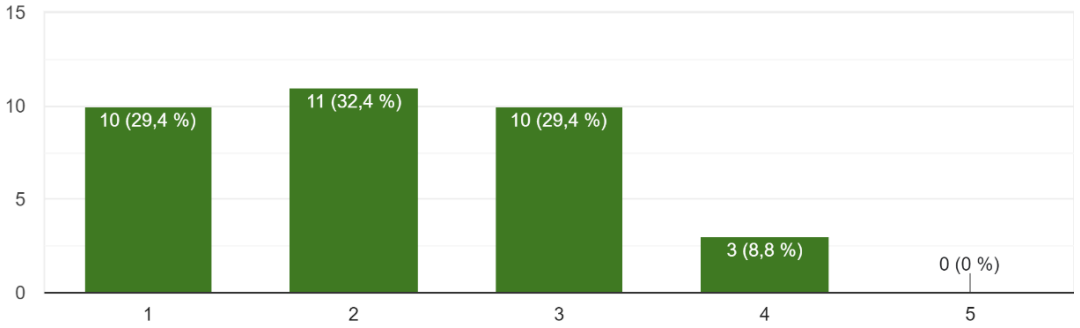


Nota. Esta figura muestra el grado de familiaridad de los encuestados con las políticas de protección de datos personales en su juzgado.

Análisis: La familiaridad con las políticas de protección de datos personales dentro del juzgado muestra una distribución predominantemente baja. Un 26.5% de los encuestados está completamente en desacuerdo con la afirmación de que están familiarizados con las políticas, y un 32.4% adicional está en desacuerdo, sugiriendo que una mayoría significativa de empleados no está adecuadamente informada sobre estas políticas. Un 17.6% se encuentra en una posición neutral, indicando una falta de certeza o conocimiento limitado. Solo el 20.6% está de acuerdo en cierta medida con la familiaridad con las políticas, y un 2.9% está totalmente de acuerdo. Esta tendencia sugiere que hay una brecha considerable en la comunicación y la comprensión de las políticas de protección de datos dentro del juzgado, lo que podría ser un área crítica a abordar para garantizar una aplicación efectiva de las normas de protección de datos.

Figura 5

Evaluación de la Efectividad de las Políticas y Procedimientos para la Protección de Datos

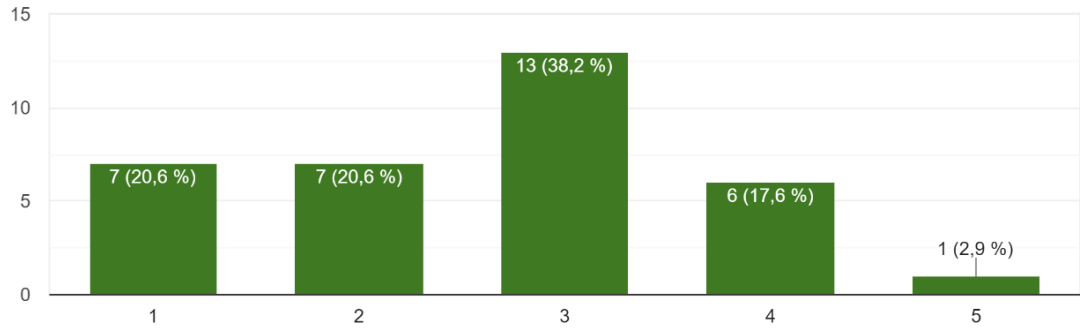


Nota. La figura ilustra la percepción de los encuestados sobre la efectividad de las políticas y procedimientos actuales para proteger los datos personales.

Análisis: La percepción sobre la efectividad de las políticas y procedimientos actuales para proteger los datos personales revela una evaluación crítica. Un 29.4% de los encuestados está completamente en desacuerdo con la afirmación de que las políticas son efectivas, mientras que otro 32.4% también está en desacuerdo, lo que indica una significativa insatisfacción con la efectividad percibida de las medidas actuales. Un 29.4% adicional se encuentra en una posición neutral, lo que sugiere incertidumbre o una evaluación mixta sobre la efectividad de las políticas. Solo el 8.8% está de acuerdo en cierta medida con la efectividad de las políticas, y ninguno está totalmente de acuerdo. Este patrón de respuestas sugiere que la mayoría de los empleados perciben que las políticas y procedimientos actuales no son suficientes para proteger adecuadamente los datos personales, destacando la necesidad urgente de revisar y fortalecer las políticas existentes.

Figura 6

Evaluación de la Efectividad de las Políticas y Procedimientos para la Protección de Datos

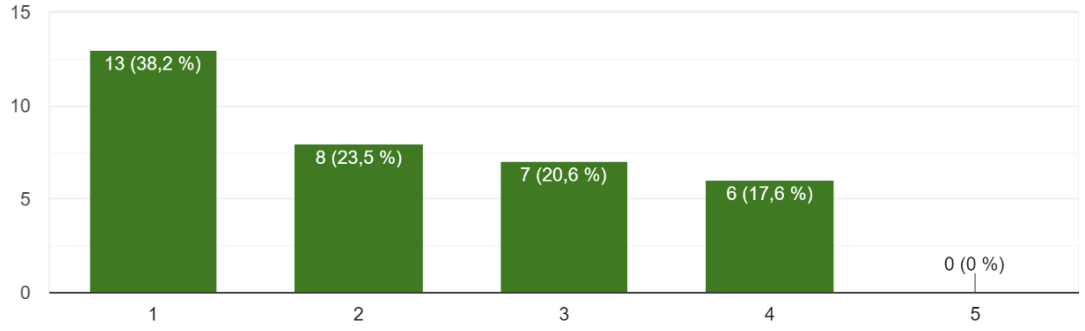


Nota. Esta figura muestra la percepción de los encuestados sobre la adecuación de la seguridad de los sistemas. La mayoría está en una posición neutral o insatisfecha sobre este tema

Análisis: La evaluación de la seguridad de los sistemas de manejo de datos personales muestra una percepción variada. Un 20.6% de los encuestados está completamente en desacuerdo con que la seguridad de los sistemas es adecuada, y otro 20.6% también está en desacuerdo, indicando preocupaciones significativas sobre la seguridad en sus lugares de trabajo. Un 38.2% se encuentra en una posición neutral, lo que puede reflejar una evaluación incierta o una falta de información clara sobre la seguridad de los sistemas. Un 20.6% está de acuerdo en cierta medida con la adecuación de la seguridad, y solo el 2.9% está totalmente de acuerdo. Esta distribución sugiere que, aunque una parte considerable de los empleados tiene dudas o preocupaciones sobre la seguridad de los sistemas de manejo de datos, existe una falta de consenso claro, lo que podría indicar una necesidad de mejoras en la percepción y la implementación de medidas de seguridad efectivas.

Figura 7

Evaluación de la Efectividad de las Políticas y Procedimientos para la Protección de Datos

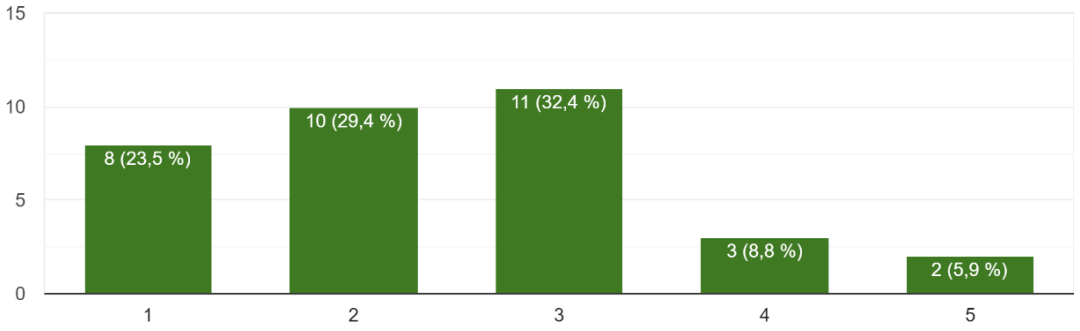


Nota. La figura representa la percepción de los encuestados sobre la efectividad de las prácticas de anonimización o pseudonimización utilizadas para proteger los datos personales

Análisis: La percepción sobre el uso de prácticas de anonimización o pseudonimización para proteger los datos personales muestra una preocupación significativa. Un 38.2% de los encuestados está completamente en desacuerdo con la afirmación de que estas prácticas se utilizan de manera efectiva, y un 23.5% también está en desacuerdo, lo que indica una percepción generalizada de que estas prácticas no se aplican adecuadamente. Un 20.6% se encuentra en una posición neutral, posiblemente debido a una falta de información clara sobre la implementación de estas prácticas. Solo el 17.6% está de acuerdo en cierta medida con la efectividad de la anonimización y pseudonimización, y ningún encuestado considera que estas prácticas se utilicen de manera completamente efectiva. Esta tendencia sugiere que existe una percepción predominante de que las prácticas de protección de datos mediante anonimización o pseudonimización son insuficientes, lo que podría indicar una necesidad urgente de revisar y mejorar estas prácticas en el manejo de datos personales.

Figura 8

Existencia de Procedimientos Claros y Eficaces para el Manejo de Brechas de Seguridad

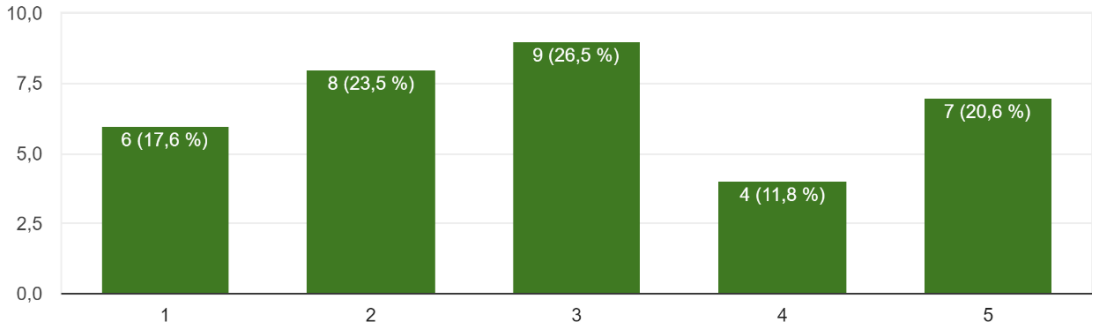


Nota. Esta figura ilustra la percepción de los encuestados sobre la existencia de procedimientos claros y eficaces para manejar brechas de seguridad o violaciones de datos personales.

Análisis: La percepción sobre la existencia de procedimientos claros y eficaces para el manejo de brechas de seguridad o violaciones de datos personales revela una evaluación crítica y variada. Un 23.5% de los encuestados está completamente en desacuerdo con la afirmación de que existen procedimientos claros y eficaces, y un 29.4% también está en desacuerdo, lo que indica una preocupación significativa por la falta de procedimientos adecuados para gestionar brechas de seguridad. Un 32.4% se encuentra en una posición neutral, lo que puede reflejar incertidumbre o falta de conocimiento sobre los procedimientos existentes. Solo el 8.8% está de acuerdo en cierta medida, y el 5.9% está completamente de acuerdo con la eficacia y claridad de los procedimientos. Esta distribución sugiere que la mayoría de los empleados perciben deficiencias en los procedimientos para manejar brechas de seguridad, destacando la necesidad de mejorar la claridad, la comunicación y la eficacia de estos procedimientos en la protección de datos personales.

Figura 9

Observación de Situaciones donde la Protección de Datos Personales Pudo Haber Sido Comprometida



Nota. La figura muestra el grado en que los encuestados han observado situaciones donde la protección de datos personales pudo haberse comprometido.

Análisis: La percepción sobre la ocurrencia de situaciones donde la protección de datos personales pudo haberse comprometido muestra una evaluación mixta pero preocupante. Un 17.6% de los encuestados está completamente en desacuerdo con haber observado tales situaciones, mientras que un 23.5% también está en desacuerdo, lo que indica que una parte de los participantes no percibe compromisos en la protección de datos. Sin embargo, un 26.5% está en una posición neutral, sugiriendo que algunos empleados tienen una visión incierta o limitada sobre posibles compromisos. Por otro lado, un 11.8% está de acuerdo en cierta medida, y un 20.6% está completamente de acuerdo en que han observado situaciones comprometedoras. Esta distribución sugiere que, aunque una parte considerable de los encuestados ha observado situaciones preocupantes relacionadas con la protección de datos, existe una falta de consenso general, lo que podría reflejar una necesidad de una mayor vigilancia y medidas proactivas para abordar y prevenir compromisos en la protección de datos personales.

Según los datos recopilados, se observa una diversidad de áreas de trabajo dentro del sistema judicial, desde el ámbito administrativo hasta el ejercicio legal en distintas ramas del derecho. Esto sugiere una amplia variedad de roles y responsabilidades en relación con la protección de datos personales. En cuanto a la experiencia laboral en el sistema judicial, se evidencia una distribución heterogénea, con periodos que van desde meses hasta décadas. Este espectro temporal puede influir en el nivel de familiarización y capacitación en temas de protección de datos.

La protección de datos personales en el contexto judicial es una preocupación creciente, dada la naturaleza sensible de la información manejada en los procesos judiciales. El Consejo de la Judicatura, como ente encargado de la administración de justicia, debe asegurar que se cumplan los más altos estándares en la protección de la privacidad y la seguridad de los datos de los ciudadanos. Con este fin, se ha realizado una investigación para evaluar el grado de conocimiento, capacitación y percepción sobre la protección de datos personales entre los empleados del sistema judicial.

1.3.1 Interpretación de los resultados:

Los resultados muestran que, si bien una parte significativa de los encuestados ha recibido formación específica sobre protección de datos personales, existe una brecha notable en la percepción de la adecuación de esta formación. Aproximadamente el 41.2% considera que la formación recibida es insuficiente, lo que destaca la necesidad de mejorar los programas de capacitación en este ámbito.

Además, aunque una mayoría significativa afirma estar familiarizada con las políticas de protección de datos de su juzgado, los niveles de confianza en la efectividad de dichas políticas y procedimientos son menos consistentes. Solo el 29.4% considera que los procedimientos actuales son efectivos para proteger los datos personales, lo que indica una percepción de vulnerabilidad o deficiencia en las medidas implementadas.

En cuanto a la seguridad de los sistemas de manejo de datos personales, aunque una parte considerable de los encuestados percibe la adecuación de las medidas de seguridad, aún hay margen de mejora, especialmente en la implementación de prácticas de anonimización o pseudonimización.

Finalmente, las sugerencias para mejorar la protección de datos personales en los procesos judiciales van desde una mayor capacitación y concientización hasta la implementación de políticas más robustas y procedimientos más claros y efectivos.

Estas sugerencias reflejan la necesidad de una revisión exhaustiva de los protocolos existentes y una mayor inversión en la formación y sensibilización del personal del sistema judicial en materia de protección de datos.

CAPÍTULO II: PROPUESTA

2.1 Fundamentos teóricos aplicados

La protección de datos personales es un derecho fundamental reconocido en diversas legislaciones a nivel mundial y en Ecuador. Este derecho garantiza que cualquier información relacionada con una persona identificada o identificable esté adecuadamente resguardada, evitando su tratamiento indebido, divulgación no autorizada o cualquier otro acto que pudiera poner en riesgo la privacidad y la integridad del titular de los datos. (Asamblea Nacional, 2021).

2.2. Marco Jurídico Internacional y Nacional

2.2.1. Reglamento General de Protección de Datos (GDPR)

El Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) de la Unión Europea es uno de los instrumentos más avanzados en materia de protección de datos. Aunque se trata de una normativa europea, sus principios y disposiciones han influenciado a nivel global, incluyendo a Ecuador. Los pilares fundamentales del GDPR, como la transparencia, la minimización de datos, el consentimiento explícito y la responsabilidad proactiva, son esenciales en cualquier sistema de protección de datos. (Asamblea Nacional, 2021).

2.2.2. Constitución de la República del Ecuador

La Constitución de Ecuador establece en su Art. 66 el derecho a la protección de datos personales, lo cual sienta la base para el desarrollo de una normativa específica en este ámbito. Además, el Art. 92 reconoce el habeas data como una herramienta jurídica para garantizar este derecho.

2.2.3. Ley Orgánica de Protección de Datos Personales (LOPDP)

La LOPDP, promulgada en 2021, establece un marco normativo integral para la protección de datos personales en Ecuador. Define conceptos fundamentales como el consentimiento, los derechos de los titulares de los datos (acceso, rectificación, cancelación, oposición), y establece las obligaciones de los responsables y encargados del tratamiento de datos. (Asamblea Nacional, 2021).

2.3. Conceptos Clave en la Protección de Datos

2.3.1. Datos Personales

Cualquier información que se relacione con una persona física identificada o identificable. Ejemplos incluyen nombres, números de identificación, datos de ubicación, identificadores en línea, entre otros.

2.3.2. Responsable del Tratamiento

La persona o entidad que decide sobre la finalidad y los medios del tratamiento de datos personales. En el contexto del Consejo de la Judicatura, esta responsabilidad recaería en la propia institución.

2.3.3. Encargado del Tratamiento

Es la persona o entidad que realiza el tratamiento de datos personales por cuenta del responsable. Debe actuar conforme a las instrucciones del responsable y cumplir con las disposiciones de la ley.

2.3.4. Principios del Tratamiento de Datos

La LOPDP establece varios principios que deben regir el tratamiento de datos personales:

- **Licitud**: El tratamiento debe ser legítimo y acorde a la normativa vigente.
- **Lealtad y Transparencia**: El manejo de los datos debe ser claro y transparente para el titular de la información.
- **Finalidad**: Los datos deben ser recogidos con propósitos específicos y legales.
- **Minimización de Datos**: Solo se deben procesar los datos que sean estrictamente necesarios para cumplir con el propósito establecido.
- **Exactitud**: Los datos deben ser exactos y estar actualizados.
- **Conservación**: Los datos no deben ser conservados más tiempo del necesario.
- **Integridad y Confidencialidad**: Se deben tomar medidas para garantizar la seguridad de los datos.

2.4. Bases Teóricas para la Aplicación en el Consejo de la Judicatura

La aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura de Ecuador se fundamenta en principios de gobernanza de la información y gestión de riesgos. Estos principios buscan garantizar la protección de los datos personales en todas las etapas de su ciclo de vida, desde la recolección hasta la eliminación. (Asamblea Nacional, 2021).

2.4.1. Gobernanza de la Información

La gobernanza de la información implica establecer políticas, procedimientos y responsabilidades claras para el tratamiento de datos personales. Esto incluye la designación de un delegado de Protección de Datos, la implementación de medidas técnicas y organizativas adecuadas, y la creación de mecanismos de supervisión y auditoría. (Asamblea Nacional, 2021).

2.4.2. Gestión de Riesgos

La gestión de riesgos es crucial para identificar, evaluar y mitigar los riesgos asociados al tratamiento de datos personales. Esto implica realizar evaluaciones de impacto, implementar controles de seguridad, y asegurar la formación continua del personal en materia de protección de datos.

2.5 Descripción de la propuesta

La propuesta se centra en el desarrollo e implementación de una Guía Integral para la aplicación de la Ley de Protección de Datos Personales en el Consejo de la Judicatura de Ecuador. Este documento servirá como un marco de referencia obligatorio para todos los actores involucrados en el tratamiento de datos personales dentro de la institución, garantizando así el cumplimiento de la normativa vigente y la protección efectiva de los datos personales de los ciudadanos.

Objetivos de la Guía

- **Cumplimiento Normativo:** Asegurar que el Consejo de la Judicatura cumpla con la Ley Orgánica de Protección de Datos Personales (LOPDP) en todas sus actividades.
- **Establecimiento de Políticas y Procedimientos:** Proporcionar directrices claras y detalladas sobre la recolección, almacenamiento, uso, y eliminación de datos personales.
- **Protección de Derechos:** Garantizar que los derechos de los titulares de los datos (acceso, rectificación, cancelación, oposición) sean respetados y facilitados por la institución.
- **Mitigación de Riesgos:** Implementar un sistema de gestión de riesgos asociado al manejo de datos personales para prevenir incidentes de seguridad y violaciones a la privacidad.
- **Capacitación y Concienciación:** Establecer un programa continuo de formación para todos los empleados del Consejo de la Judicatura, asegurando que estén informados sobre sus responsabilidades y adopten las mejores prácticas para proteger los datos.

2.6 Estructura general

La Guía para la Aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura es un marco integral diseñado para garantizar el cumplimiento normativo y la protección de los datos personales en todas las operaciones de la institución.

En la figura 10 se puede observar la guía que establece las políticas, procedimientos, y protocolos claros para la recolección, manejo, y almacenamiento de datos, asegurando la minimización de riesgos y la protección de los derechos de los titulares. A través de un enfoque estructurado, la guía facilita la formación continua del personal, la evaluación de impactos y la

gestión de incidentes, promoviendo una cultura institucional de respeto a la privacidad y seguridad de la información.

Figura 10

Estructura general de la Guía para la Aplicación de la Ley de Protección de Datos

Nota. Aquí se puede observar todas las fases que contiene y se van a desarrollar dentro de la Guía para la Aplicación de la Ley de Protección de Datos

2.6.1 Explicación del aporte

El aporte principal de la Guía para la Aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura radica en el fortalecimiento de la protección de datos personales tanto dentro de la institución como en su interacción con la sociedad. Esta guía no solo asegura el cumplimiento de la normativa vigente, sino que también promueve una cultura de privacidad y seguridad en el manejo de la información sensible. Como resultado, se espera que la confianza del público en el sistema judicial se incremente, mejorando la percepción y legitimidad del Consejo de la Judicatura.

2.7 Funcionamiento y Empleo de Cada Componente de la Propuesta

I. Introducción

- **Funcionamiento:** Establece el contexto y propósito de la guía, explicando la relevancia de la protección de datos en el ámbito judicial.
- **Empleo:** Utilizado como punto de partida para comprender la necesidad y los objetivos de la guía dentro del Consejo de la Judicatura.

II. Marco Legal y Normativo

- **Funcionamiento:** Proporciona un resumen del marco jurídico relevante, incluyendo la Ley de Protección de Datos y otras normativas aplicables.
- **Empleo:** Sirve como referencia legal para asegurar que todas las acciones del Consejo cumplan con la normativa vigente, orientando a los responsables en el manejo de datos personales.

III. Roles y Responsabilidades

- **Funcionamiento:** Define claramente los actores involucrados y sus respectivas responsabilidades en la protección de datos.
- **Empleo:** Asigna tareas específicas y designa responsables de protección de datos, garantizando que cada miembro del Consejo entienda su papel en la salvaguarda de la información personal.

IV. Formación y Concientización

- **Funcionamiento:** Establece programas de capacitación y sensibilización para el personal del Consejo de la Judicatura.
- **Empleo:** Asegura que todos los empleados estén bien informados sobre las mejores prácticas de protección de datos y que se mantengan actualizados sobre cambios normativos.

V. Políticas y Procedimientos

- **Funcionamiento:** Desarrolla políticas internas y procedimientos estandarizados para el tratamiento de datos personales.
- **Empleo:** Proporciona directrices claras sobre cómo se deben manejar los datos personales en la institución, incluyendo protocolos de seguridad y procesamiento de datos.

VI. Seguridad de los Sistemas y Datos

- **Funcionamiento:** Establece las medidas técnicas y organizativas requeridas para salvaguardar los sistemas y datos del Consejo.
- **Empleo:** Implementa protecciones contra accesos no autorizados, ciberataques y gestiona incidentes de seguridad para mantener la integridad y privacidad de la información

VII. Auditoría y Monitoreo

- **Funcionamiento:** Establece procesos de auditoría interna y monitoreo continuo para asegurar el cumplimiento de la guía.
- **Empleo:** Permite la identificación de riesgos y vulnerabilidades en el sistema, asegurando que se tomen medidas correctivas para mantener la seguridad de los datos.

VIII. Gestión de Incidentes

- **Funcionamiento:** Proporciona un protocolo para la gestión de incidentes de seguridad, incluyendo la notificación de violaciones de datos.
- **Empleo:** Asegura una respuesta rápida y eficaz ante cualquier incidente, minimizando el impacto y aplicando medidas correctivas oportunas.

IX. Evaluación y Mejora Continua

- **Funcionamiento:** Establece un proceso para la evaluación periódica y mejora continua de las políticas y procedimientos de protección de datos.
- **Empleo:** Facilita la adaptación de la guía a nuevos desafíos legales y tecnológicos, asegurando su relevancia y efectividad a lo largo del tiempo.

X. Conclusiones

- **Funcionamiento:** Resume los puntos clave de la guía y refuerza la importancia de su aplicación efectiva.
- **Empleo:** Se utiliza para reafirmar el compromiso del Consejo de la Judicatura con la privacidad y seguridad de los datos personales, promoviendo la confianza del público en la institución.

2.8 Estrategias y/o técnicas

La Guía para la Aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura se fundamenta en una serie de estrategias y técnicas que aseguran su efectividad y cumplimiento. A continuación, se detallan los elementos, metodologías, técnicas, y estándares utilizados en cada una de las evaluaciones propuestas.

2.8.1 Evaluación de Impacto en la Protección de Datos (EIPD)

- **Elemento:** Análisis de riesgos asociados al tratamiento de datos personales.
- **Metodología:** Realización de una evaluación exhaustiva de los posibles impactos que las actividades de tratamiento de datos puedan tener sobre los derechos y libertades de los titulares de los datos.
- **Técnicas:**
    - **Identificación de riesgos:** Se identifican y describen los riesgos potenciales.
    - **Análisis de probabilidad e impacto:** Se evalúa la probabilidad de que cada riesgo ocurra y su impacto potencial.
    - **Planificación de medidas de mitigación:** Desarrollo de estrategias para reducir la probabilidad y el impacto de los riesgos identificados.
- **Estándares:** Basado en las directrices del Reglamento General de Protección de Datos (GDPR) y las mejores prácticas internacionales en privacidad de datos.

2.8.2 Auditoría Interna de Cumplimiento

- **Elemento:** Revisión sistemática del cumplimiento con las políticas y procedimientos establecidos en la guía.
- **Metodología:** Realización de auditorías periódicas para verificar la adherencia a los estándares de protección de datos.
- **Técnicas:**
    - **Revisión documental:** Evaluación de políticas, registros y documentación relacionada con la protección de datos.
    - **Entrevistas:** Realización de entrevistas con el personal clave para evaluar su conocimiento y cumplimiento de las políticas.
    - **Pruebas de cumplimiento:** Ejecución de pruebas específicas para verificar la correcta implementación de las políticas y procedimientos.
- **Estándares:** Normas ISO 19011 para la auditoría de sistemas de gestión y la ISO/IEC 27001 para la gestión de la seguridad de la información.

2.8.3 Monitoreo Continuo de la Seguridad de los Datos

- **Elemento:** Supervisión constante de los sistemas y datos para identificar vulnerabilidades y amenazas en tiempo real.
- **Metodología:** Implementación de sistemas de monitoreo automatizado y análisis continuo de logs y eventos de seguridad.
- **Técnicas:**
    - **Monitoreo de eventos de seguridad:** Utilización de herramientas como SIEM (Security Information and Event Management) para centralizar y analizar eventos de seguridad.
    - **Análisis de vulnerabilidades:** Uso de herramientas de escaneo de vulnerabilidades para identificar puntos débiles en los sistemas de TI.
    - **Alertas en tiempo real:** Configuración de alertas para notificar inmediatamente cualquier actividad sospechosa o incumplimiento.
- **Estándares:** Normas ISO/IEC 27002 para la implementación de controles de seguridad de la información.

2.8.4 Gestión de Incidentes de Seguridad

- **Elemento:** Procedimientos para la identificación, análisis, y respuesta a incidentes de seguridad que afecten la protección de datos personales.
- **Metodología:** Desarrollo e implementación de un plan de respuesta a incidentes que incluya identificación, contención, erradicación, recuperación, y lecciones aprendidas.
- **Técnicas:**
    - **Detección de incidentes:** Implementación de herramientas y procesos para identificar rápidamente incidentes de seguridad.
    - **Análisis forense:** Realización de análisis forense digital para entender la causa raíz de los incidentes y su impacto.
    - **Notificación de incidentes:** Procedimientos para informar a las autoridades y a los titulares de los datos en caso de una brecha significativa en la seguridad.
- **Estándares:** NIST SP 800-61 para la gestión de incidentes de seguridad informática.

2.8.5 Evaluación Periódica de la Efectividad de las Medidas de Protección

- **Elemento:** Revisión regular de la efectividad de las políticas, procedimientos y controles implementados.
- **Metodología:** Realización de evaluaciones periódicas que analicen el desempeño de las medidas de protección y su alineación con los objetivos de la guía.

- **Técnicas:**
    - **Revisión de indicadores de rendimiento (KPIs):** Establecimiento y seguimiento de KPIs relacionados con la protección de datos.
    - **Encuestas de satisfacción:** Realización de encuestas para medir la satisfacción de los titulares de los datos respecto al manejo de su información.
    - **Análisis de brechas:** Identificación de diferencias entre las prácticas actuales y las mejores prácticas o estándares establecidos.
- **Estándares:** ISO/IEC 27004 para la medición del rendimiento de los sistemas de gestión de la seguridad de la información.

2.9 Validación de la propuesta

La validación de la Guía para la Aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura es un paso crucial para asegurar su efectividad y aplicabilidad. Para este fin, se utilizará el método de criterios de especialistas, en el cual se busca la opinión de expertos en áreas relevantes para garantizar que la propuesta cumple con los estándares y prácticas de la industria.

2.10 Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 1.
Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Contexto Legal y Tecnológico	Constitución de la República del Ecuador, OEA	Investigación documental y revisión normativa	Análisis de contenido, revisión de literatura	Identificación de los derechos y obligaciones relacionados con la protección de datos personales	Documentos legales, artículos académicos
Protección de Datos Personales	Principios de privacidad y protección de datos (OEA, Consejo de Europa)	Análisis de casos y legislación comparada	Estudios de caso, análisis comparativo	Comparación de normativas y principios en diferentes jurisdicciones	Informes de casos, comparaciones legislativas

Autorización del Titular de los Datos	Doctrina sobre el consentimiento informado y derechos digitales	Encuestas	Encuestas	Recopilación de opiniones y prácticas actuales en la autorización de datos	Cuestionarios, guías de entrevistas
Sistema Ecuatoriano de Trámite Judicial	Principio de publicidad y derecho a la privacidad	Análisis de jurisprudencia y prácticas judiciales	Revisión de casos judiciales, análisis normativo	Evaluación del equilibrio entre publicidad y privacidad en el sistema judicial	Expedientes judiciales, normativas aplicables
Derechos Digitales	Guía de Derechos Humanos para los Usuarios de Internet (Consejo de Europa)	Análisis de políticas y regulación digital	Revisión de políticas, análisis de impacto	Identificación de derechos y protección en el entorno digital	Políticas digitales, guías de derechos

Nota: Elaboración propia

CONCLUSIONES

La revisión de los fundamentos teóricos básicos sobre el tratamiento de datos personales conforme a la Ley Orgánica de Protección de Datos Personales proporciona una base sólida para entender los principios y requisitos legales aplicables. Esta contextualización es crucial para asegurar que cualquier estrategia o acción relacionada con la protección de datos esté alineada con las normativas vigentes y garantice el cumplimiento adecuado de las leyes de privacidad.

El diagnóstico de la situación actual del Consejo de la Judicatura en relación con la Ley de Protección de Datos revela el nivel de implementación y cumplimiento de esta legislación en el ámbito judicial. Este análisis es esencial para identificar posibles brechas o áreas de mejora en la protección de datos dentro del sistema judicial, facilitando así el desarrollo de estrategias y recomendaciones específicas para optimizar el manejo de datos personales en el contexto de procesos judiciales.

El diseño de la guía para la solicitud de protección de datos personales de personas involucradas en procesos judiciales penalmente sobreseídos o con sentencias ratificatorias de inocencia es un paso fundamental para ofrecer claridad y facilidad en el proceso de protección de datos. Esta guía pretende proporcionar un marco práctico y accesible para que las personas afectadas puedan ejercer sus derechos de manera efectiva, contribuyendo así a una mayor transparencia y protección en la gestión de datos personales judiciales.

La validación de la guía mediante la revisión de especialistas jurídicos en materia constitucional y legal asegura que el documento cumpla con los estándares legales y constitucionales requeridos. Este proceso de validación es crucial para garantizar que la guía sea jurídicamente sólida, efectiva y aplicable en la práctica, además de proporcionar confianza en su uso por parte de los ciudadanos y las instituciones.

En resumen, estos objetivos contribuyen a una comprensión integral y a la mejora continua en el manejo de datos personales en el contexto judicial, promoviendo un enfoque informado y conforme a la ley para la protección de la privacidad de los individuos involucrados en procesos judiciales.

RECOMENDACIONES

Se recomienda analizar de manera precisa todo el contenido dado acerca de la Ley de Protección de datos, desde el Art 1 citado en la introducción.

Es recomendable mantenerse siempre informado e investigando acerca de la LPDP debido a que siempre pueden existir modificaciones en la Ley.

Es recomendable que se revise todo el trabajo realizado y el Plan detallado, de ser necesario seguir en proceso de mejora y acoplamiento de la seguridad informática y la Ley de protección de datos.

Se recomienda utilizar métodos investigativos para el desarrollo de cualquier trabajo de titulación debido a que sus herramientas brindarán la facilidad en la obtención de resultados favorables para la investigación.

Bibliografía

Bibliografía

Asamblea Nacional. (26 de 05 de 2021). *Ley organica de proteccion de datos personales* . Obtenido de Ley organica de proteccion de datos personales : https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf&ved=2ahUKEwi74M74tpWIAxUuj4QIHYoNGi4QFnoECBoQAQ&usg=AOvVaw14qxux2y-WUfOEm4

Alonso, C. (2021). *Claves de la Ley Orgánica de Protección de Datos Personales de Ecuador*. Obtenido de https://www.globalsuitesolutions.com/es/claves-proyecto-ley-organica-proteccion-de-datos-personales-ecuador/

Alonso, C. (2021). *Claves de la Ley Orgánica de Protección de Datos Personales de Ecuador*. Obtenido de https://www.globalsuitesolutions.com/es/claves-proyecto-ley-organica-proteccion-de-datos-personales-ecuador/

Asamblea Nacional. (26 de 05 de 2021). *Ley organica de proteccion de datos personales*. Obtenido de Ley organica de proteccion de datos personales : https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf&ved=2ahUKEwi74M74tpWIAxUuj4QIHYoNGi4QFnoECBoQAQ&usg=AOvVaw14qxux2y-WUfOEm4

Arellano, C. (2020). El derecho de protección de datos personales. *Biolex*, 163-174.

doi:https://doi.org/10.36796/biolex.v0i23.194

Encuesta. (2020). Obtenido de

http://bivicce.corteconstitucional.gob.ec/bases/biblo/texto/TRC/46-01.pdf

Hernández Alvarado, V. J., Pingel Llanos, O. F., & Coello Avilés, E. M. (2023). Ley Orgánica de Protección de Datos en Ecuador: requerimiento de un reglamento ausente. Revista Dilemas Contemporáneos: Educación, Política y Valores, XI(Edición Especial), Artículo no. 114. Recuperado de https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/download/3988/3904/

Instituto de la Juventud. (2016). *Orientaciones*. Obtenido de Orientaciones: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.injuve.es/sites/default/files/2019/07/publicaciones/orientaciones.pdf&ved=2ahUKEwidydzyupWIAxVvTDABHWZvMbYQFnoECBQQAQ&usg=AOvVaw0XNgw9thOC_5SMeMRkSc-D

Introducción del problema. (s.f.). Obtenido de https://www.primicias.ec/noticias/economia/ley-proteccion-datos-multas-funcionarios/

J. Casas Anguita, J. R. (28 de 01 de 2002). *La encuesta como tecnicas de investigacion*. Obtenido de https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://core.ac.uk/download/pdf/82245762.pdf&ved=2ahUKEwjd8MSkvJWIAxWMtYQIHdSuESIQFnoECBcQAQ&usg=AOvVaw0-fHcH6d4TYx-Og5_rZiL7

Ley de protección. (s.f.). Obtenido de https://www.coface.com.ec/Home/Informacion-General/Preguntas-Frecuentes-RGPD.

Ley de protección. (26 de 05 de 2021). Obtenido de Ley de protección: https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Ley de protección de datos. (18 de 07 de 2023). Obtenido de Ley de protección de datos: https://russellbedford.com.ec/ley-de-proteccion-de-datos-personales-en-ecuador/

Martínez, S. N. (s.f.). Obtenido de https://nmslaw.com.ec/ley-organica-proteccion-datos-personales

Miralles, R. (2010). Cloud computing y protección de datos. IDP Número 11, 1699-8154. Recuperado de https://openaccess.uoc.edu/bitstream/10609/8699/1/miralles-esp.pdf

Principios actualizados sobre la privacidad y la proteccion de datos personales. (31 de 05 de 2019). Obtenido de Principios actualizados sobre la privacidad y la proteccion de datos personales:https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf&ved=2ahUKEwj7wsPluZWIAxWbpLAFHYM4ElkQFnoECBkQAQ&usg=AOvVaw3E58ORpvIOqYVx_5B52YmT

Protección de datos. (5 de 07 de 2024). Obtenido de https://biblioguias.cepal.org/c.php?g=495473&p=4398118

Sector Publico. (s.f.). Obtenido de https://www.bizkaia.eus/es/web/educacion-tributaria/sector-publico

Servidor público. (s.f.). Obtenido de https://www.finanzas.gob.ec/wp-content/uploads/downloads/2012/09/LEY_SERVICIO_PUBLICO.pdf

Anexo 1

La Guía para la Aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura se fundamenta en una serie de estrategias y técnicas que aseguran su efectividad y cumplimiento. A continuación, se detallan los elementos, metodologías, técnicas, y estándares utilizados en cada una de las evaluaciones propuestas.

Guía para la Aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura

I. Introducción

- **Propósito de la guía.**

Esta guía tiene como propósito proporcionar una orientación clara y práctica para la aplicación de la Ley de Protección de Datos Personales dentro del Consejo de la Judicatura. Su objetivo es asegurar que todas las actividades relacionadas con el tratamiento de datos personales en el ámbito judicial se realicen de manera legal, ética y segura, protegiendo los derechos de las personas y garantizando la transparencia y la confianza en el sistema judicial.

- **Contexto del Consejo de la Judicatura.**

El Consejo de la Judicatura es el órgano encargado de la administración de la justicia, supervisión de jueces y tribunales, y la organización y gestión de los recursos necesarios para el adecuado funcionamiento del sistema judicial. En este contexto, el Consejo maneja una gran cantidad de información personal y sensible, incluyendo datos de ciudadanos, funcionarios judiciales, y otras partes interesadas, lo que hace imperativa una correcta aplicación de la normativa de protección de datos.

Importancia de la protección de datos personales en el ámbito judicial.

La protección de datos personales es crucial en el ámbito judicial debido a la naturaleza delicada y confidencial de la información manejada. Una adecuada gestión de estos datos no solo es un mandato legal, sino también una obligación ética que contribuye a la confianza pública en el sistema judicial.

El incumplimiento de las normas de protección de datos puede llevar a graves consecuencias, tanto legales como reputacionales, afectando la integridad del Consejo y los derechos de las personas implicadas.

II. Marco Legal y Normativo

Ley de Protección de Datos y su aplicación en el sistema judicial.

La Ley de Protección de Datos Personales establece el marco legal para el tratamiento adecuado de la información personal en todas las esferas, incluyendo el ámbito judicial. En el contexto del Consejo de la Judicatura, esta ley es fundamental para garantizar que los datos personales de ciudadanos, empleados, y otras partes involucradas en procesos judiciales sean manejados de manera segura, confidencial, y en conformidad con los principios de legalidad, consentimiento, finalidad, calidad, proporcionalidad, y responsabilidad.

La aplicación de esta ley en el sistema judicial implica que todas las actividades relacionadas con la recopilación, almacenamiento, procesamiento, y divulgación de datos personales deben cumplir con los estándares establecidos para proteger los derechos de los individuos, evitando accesos no autorizados, alteraciones, pérdidas, y otras formas de tratamiento indebido de la información.

Reglamentos y normativas complementarias.

Además de la Ley de Protección de Datos, existen reglamentos y normativas complementarias que guían su implementación específica dentro del Consejo de la Judicatura. Estos incluyen:

Reglamentos Internos del Consejo de la Judicatura: Establecen procedimientos específicos para el manejo de datos personales en el contexto judicial, incluyendo medidas de seguridad, protocolos de acceso a la información, y políticas de retención y eliminación de datos.

Directrices del Organismo de Supervisión de Protección de Datos: Instrucciones y recomendaciones emitidas por el organismo regulador encargado de la protección de datos personales en el país, que orientan al Consejo en la correcta aplicación de la normativa.

Normas Técnicas de Seguridad: Normas que establecen los requisitos mínimos de seguridad informática y física que deben cumplirse para proteger los sistemas de información y los datos personales almacenados en ellos.

Responsabilidades del Consejo de la Judicatura en la protección de datos.

El Consejo de la Judicatura tiene varias responsabilidades clave en la protección de datos personales:

Designación de un Delegado de Protección de Datos (DPD): Una figura responsable de supervisar la correcta aplicación de la normativa de protección de datos, asesorar al Consejo en materia de privacidad, y actuar como punto de contacto con el organismo regulador y con los titulares de datos.

Implementación de Políticas y Procedimientos de Protección de Datos: Desarrollo e implementación de políticas internas que aseguren el cumplimiento de la ley, incluyendo procedimientos para la gestión de brechas de seguridad, solicitudes de acceso por parte de los titulares de datos, y la realización de evaluaciones de impacto de protección de datos (EIPD).

Capacitación y Concienciación: Asegurar que todos los empleados y funcionarios del Consejo estén debidamente capacitados en materia de protección de datos personales, comprendan sus responsabilidades, y conozcan las mejores prácticas para proteger la información a la que tienen acceso.

Monitoreo y Auditoría: Realizar monitoreos y auditorías regulares para evaluar la efectividad de las medidas de protección de datos implementadas, identificar riesgos potenciales, y realizar ajustes necesarios para garantizar la seguridad y el cumplimiento continuo de la normativa.

III. Roles y Responsabilidades

Identificación de actores y sus funciones en la protección de datos.

En el Consejo de la Judicatura, la protección de datos personales requiere la colaboración de múltiples actores, cada uno con responsabilidades específicas:

Consejo de la Judicatura: Como órgano rector, el Consejo es responsable de establecer y supervisar la implementación de políticas y procedimientos de protección de datos en todo el sistema judicial.

Delegado de Protección de Datos (DPD): Responsable de velar por el cumplimiento de la normativa de protección de datos, asesorar al Consejo y a sus dependencias, y actuar como enlace con las autoridades de control y con los titulares de los datos.

Personal Judicial: Incluye jueces, secretarios, abogados, y demás empleados que manejan información personal en sus labores diarias. Son responsables de cumplir con las políticas de protección de datos y de asegurar que el tratamiento de la información se realice de manera legal y ética.

Terceros y Proveedores de Servicios: Entidades externas que, en ocasiones, manejan datos personales en nombre del Consejo. Estos actores deben estar sujetos a acuerdos de

confidencialidad y a cumplir con los estándares de protección de datos establecidos por el Consejo.

Obligaciones del personal judicial.

El personal judicial tiene la obligación de:

Cumplir con la Ley de Protección de Datos y Normativas Internas: Todos los funcionarios deben asegurarse de que el tratamiento de datos personales cumpla con la normativa vigente y las políticas internas del Consejo.

Mantener la Confidencialidad de los Datos: El personal debe garantizar la confidencialidad de la información a la que tienen acceso, evitando divulgaciones no autorizadas y adoptando las medidas necesarias para proteger la privacidad de los datos.

Reportar Incidentes de Seguridad: Cualquier sospecha de violación de datos, acceso no autorizado, o pérdida de información debe ser reportada de inmediato al delegado de Protección de Datos o al responsable designado.

Participar en Programas de Capacitación: Es obligación del personal mantenerse actualizado sobre las mejores prácticas de protección de datos a través de programas de formación y concienciación proporcionados por el Consejo.

Designación de responsables de protección de datos.

El Consejo de la Judicatura debe designar responsables claros para la protección de datos en diferentes niveles:

Delegado de Protección de Datos (DPD): Un profesional cualificado que actúa como el principal garante del cumplimiento de la normativa de protección de datos. Este delegado supervisa las políticas de protección de datos y garantiza la conformidad con las leyes aplicables.

Responsables de Área: Dentro de cada unidad o departamento del Consejo, se deben designar personas responsables de asegurar que las políticas de protección de datos se implementen correctamente. Estas personas actúan como puntos de contacto para el DPD y tienen la tarea de monitorear el cumplimiento en su respectivo ámbito.

Equipo de Respuesta a Incidentes: Un grupo de personas designadas para gestionar cualquier incidente de seguridad relacionado con la protección de datos, como brechas de seguridad o accesos no autorizados. Este equipo es responsable de coordinar las acciones correctivas y de mitigar los impactos.

IV. Formación y Concientización

Programas de capacitación sobre protección de datos.

Para asegurar un manejo adecuado de la información personal, el Consejo de la Judicatura debe implementar programas de capacitación dirigidos a todo el personal judicial. Estos programas deben cubrir:

Fundamentos de la Protección de Datos: Introducción a los conceptos básicos de privacidad, derechos de los titulares de datos, y las obligaciones legales en el tratamiento de información personal.

Políticas y Procedimientos Internos: Formación específica sobre las políticas de protección de datos del Consejo, incluyendo el manejo de datos sensibles, procedimientos de acceso y rectificación, y gestión de incidentes de seguridad.

Técnicas de Seguridad: Capacitación en medidas técnicas y organizativas para proteger la información, como el uso de contraseñas seguras, encriptación de datos, y manejo seguro de dispositivos electrónicos.

Estos programas deben ser obligatorios para todos los empleados y repetidos periódicamente para asegurar el conocimiento continuo y actualizado.

Sensibilización sobre la importancia de la privacidad.

Además de la capacitación formal, es crucial sensibilizar al personal sobre la importancia de la privacidad y la protección de datos personales en el ámbito judicial. Esto se puede lograr mediante:

Campañas de Concientización: Implementación de campañas internas que incluyan carteles, boletines informativos, y mensajes electrónicos que recuerden al personal la importancia de proteger la información personal.

Charlas y Talleres: Organizar charlas y talleres periódicos con expertos en protección de datos que puedan abordar casos prácticos y responder preguntas del personal sobre situaciones reales que puedan enfrentar en su trabajo diario.

Cultura Organizacional: Fomentar una cultura de respeto por la privacidad dentro del Consejo, donde la protección de datos se vea no solo como una obligación legal, sino como un valor fundamental que guía todas las actividades judiciales.

Actualización periódica del personal sobre cambios normativos.

La legislación en materia de protección de datos y las normativas asociadas están en constante evolución. Para garantizar el cumplimiento continuo, el Consejo de la Judicatura debe establecer mecanismos de actualización periódica del personal, tales como:

Boletines de Actualización Normativa: Distribuir regularmente boletines informativos que resuman los cambios recientes en la legislación de protección de datos, así como en reglamentos y directrices aplicables al ámbito judicial.

Sesiones de Actualización: Organizar sesiones de actualización obligatorias cada vez que se produzcan cambios significativos en la normativa o en las políticas internas del Consejo. Estas sesiones deben incluir explicaciones detalladas sobre cómo los cambios afectan el trabajo diario y qué nuevas medidas deben adoptarse.

Acceso a Recursos: Proporcionar acceso a recursos en línea, como cursos, guías, y foros de discusión, donde el personal pueda obtener más información sobre las últimas tendencias y mejores prácticas en protección de datos.

V. Políticas y Procedimientos

Desarrollo de políticas internas de protección de datos.

El Consejo de la Judicatura debe desarrollar y adoptar políticas internas claras y específicas para la protección de datos personales, que sirvan como directrices para todos los procesos y actividades relacionadas con el tratamiento de información. Estas políticas deben incluir:

Política de Privacidad: Un documento que defina cómo se recopilan, utilizan, almacenan, y protegen los datos personales dentro del Consejo. Debe incluir los derechos de los titulares de datos, las obligaciones del Consejo, y los mecanismos de control y supervisión.

Política de Retención y Eliminación de Datos: Directrices sobre cuánto tiempo se almacenarán los datos personales y los procedimientos para su eliminación segura una vez que ya no sean necesarios, asegurando que se cumplan con las regulaciones de retención aplicables.

Política de Consentimiento: Procedimientos para obtener, documentar y gestionar el consentimiento informado de los titulares de datos, asegurando que comprendan cómo se utilizará su información y que puedan retirar su consentimiento en cualquier momento.

Procedimientos para la recopilación, almacenamiento y procesamiento de datos.

Para asegurar el cumplimiento de la Ley de Protección de Datos, el Consejo debe implementar procedimientos específicos para cada etapa del ciclo de vida de la información:

Recopilación de Datos:

Limitación de Datos: Recoger únicamente los datos personales que sean estrictamente necesarios para cumplir con los fines judiciales, minimizando la recolección de información excesiva.

Transparencia: Informar a los titulares de datos sobre la finalidad de la recopilación, el uso previsto de la información, y los derechos que les asisten en relación con sus datos personales.

Almacenamiento de Datos:

Seguridad Física y Digital: Implementar medidas de seguridad robustas para proteger los datos almacenados, como controles de acceso restringidos, cifrado de archivos sensibles, y almacenamiento seguro en servidores protegidos.

Acceso Controlado: Asegurar que solo el personal autorizado tenga acceso a los datos personales, mediante mecanismos de autenticación fuertes y la asignación de permisos de acceso basados en roles.

Procesamiento de Datos:

Exactitud y Actualización: Establecer procedimientos para verificar la exactitud de los datos procesados y garantizar su actualización periódica.

Minimización de Datos: Limitar el procesamiento de datos al mínimo necesario para cumplir con los objetivos específicos, evitando el uso o procesamiento adicional no autorizado.

Protocolos de seguridad de la información.

Para proteger los datos personales manejados por el Consejo de la Judicatura, es esencial establecer protocolos de seguridad rigurosos que abarquen tanto la seguridad de la información como la seguridad física:

Seguridad Informática:

Cifrado de Datos: Implementar cifrado tanto en tránsito como en reposo para proteger los datos personales contra accesos no autorizados.

Copia de Seguridad y Recuperación: Establecer sistemas de respaldo regulares y planes de recuperación ante desastres para garantizar la integridad y disponibilidad de los datos en caso de incidentes.

Monitoreo y Detección de Intrusiones: Implementar herramientas de monitoreo continuo y detección de intrusiones para identificar y responder rápidamente a posibles amenazas de seguridad.

Seguridad Física:

Controles de Acceso: Restringir el acceso físico a las áreas donde se almacenan y procesan datos personales mediante sistemas de seguridad, como tarjetas de acceso, cámaras de vigilancia, y guardias de seguridad.

Gestión de Dispositivos: Controlar y monitorizar el uso de dispositivos que acceden a los datos personales, como ordenadores, discos duros, y dispositivos móviles, asegurando que se utilicen de manera segura y que estén protegidos contra pérdidas o robos.

Gestión de Incidentes de Seguridad:

Plan de Respuesta a Incidentes: Desarrollar y mantener un plan detallado para responder a incidentes de seguridad relacionados con la protección de datos, incluyendo procedimientos para la notificación de brechas de seguridad a las autoridades pertinentes y a los afectados.

Evaluación de Impacto: Realizar evaluaciones de impacto de protección de datos (EIPD) antes de implementar nuevos sistemas o procesos que involucren datos personales, para identificar y mitigar riesgos potenciales.

VI. Seguridad de los Sistemas y Datos

Medidas técnicas y organizativas para garantizar la seguridad y para proteger la información personal manejada por el Consejo de la Judicatura, es esencial implementar tanto medidas técnicas como organizativas que aseguren la integridad, confidencialidad y disponibilidad de los datos:

Medidas Técnicas:

Cifrado de Datos: Todos los datos personales deben ser cifrados tanto en tránsito (cuando se transmiten entre sistemas) como en reposo (cuando se almacenan), utilizando algoritmos de cifrado robustos que cumplan con los estándares internacionales.

Autenticación y Control de Acceso: Implementar sistemas de autenticación multifactor (MFA) para acceder a los sistemas que manejan datos personales, y establecer controles de acceso basados en roles, garantizando que solo el personal autorizado pueda acceder a la información.

Actualización y Parches de Seguridad: Mantener todos los sistemas y software actualizados con los últimos parches de seguridad, para protegerlos contra vulnerabilidades conocidas.

Monitoreo y Auditoría: Establecer mecanismos de monitoreo continuo de los sistemas para detectar actividades sospechosas o no autorizadas, y realizar auditorías regulares para evaluar el cumplimiento de las políticas de seguridad.

Protección contra accesos no autorizados y ciberataques.

Dado el valor y la sensibilidad de los datos manejados por el Consejo de la Judicatura, es crucial proteger los sistemas contra accesos no autorizados y ciberataques mediante las siguientes medidas:

Firewalls y Sistemas de Prevención de Intrusiones (IPS): Implementar firewalls robustos para filtrar el tráfico de red no deseado y sistemas de prevención de intrusiones que detecten y bloqueen intentos de acceso no autorizado.

Seguridad en el Endpoint: Proteger todos los dispositivos que acceden a la red del Consejo (computadoras, dispositivos móviles, etc.) con software antivirus, herramientas de detección de malware, y configuraciones de seguridad adecuadas.

Redes Seguras: Asegurar que las redes internas sean seguras mediante el uso de VLANs (Virtual Local Area Networks), segmentación de la red, y cifrado de la comunicación entre dispositivos.

Copia de Seguridad y Redundancia: Realizar copias de seguridad regulares de todos los datos críticos y almacenar esas copias en ubicaciones seguras y separadas, para asegurar la recuperación de la información en caso de un ataque de ransomware u otro incidente.

Gestión de incidentes de seguridad y brechas de datos.

La respuesta rápida y eficaz a incidentes de seguridad es esencial para minimizar el impacto de cualquier brecha de datos. El Consejo de la Judicatura debe contar con un plan integral de gestión de incidentes que incluya:

Plan de Respuesta a Incidentes:

Detección y Notificación: Establecer procedimientos para la detección inmediata de incidentes de seguridad y la notificación interna rápida al equipo de respuesta a incidentes.

Contención y Erradicación: Implementar medidas para contener el incidente y evitar su propagación, seguido de la erradicación de la causa raíz, ya sea mediante la eliminación de malware, la reparación de vulnerabilidades, o la reconfiguración de sistemas afectados.

Recuperación: Restablecer los sistemas y servicios a su estado normal lo más rápido posible, utilizando copias de seguridad y verificando la integridad de los datos restaurados.

Notificación de Brechas de Datos:

Notificación a las Autoridades: En caso de una brecha de datos que comprometa la información personal, notificar a la autoridad reguladora de protección de datos dentro del plazo establecido por la ley.

Notificación a los Afectados: Informar a los titulares de datos afectados por la brecha sobre la naturaleza del incidente, las medidas adoptadas para mitigar los daños, y las recomendaciones para protegerse contra posibles consecuencias.

Lecciones Aprendidas y Mejora Continua: Después de cada incidente, realizar un análisis exhaustivo para identificar las lecciones aprendidas, ajustar las políticas y procedimientos, y reforzar las medidas de seguridad para prevenir futuros incidentes.

VII. Auditoría y Monitoreo

Realización de auditorías internas periódicas de cumplimiento en el Consejo de la Judicatura para evaluar el cumplimiento de las políticas de protección de datos y la normativa aplicable. Estas auditorías deben incluir:

Revisión de Políticas y Procedimientos: Verificación de que las políticas internas de protección de datos están actualizadas y alineadas con las leyes y reglamentos vigentes. Se debe evaluar la efectividad de los procedimientos establecidos para la recopilación, almacenamiento, y procesamiento de datos personales.

Cumplimiento de Normas y Regulaciones: Evaluación del cumplimiento con la Ley de Protección de Datos, reglamentos específicos del sector judicial, y cualquier normativa adicional aplicable. Esto incluye la revisión de la documentación de consentimiento, políticas de retención de datos, y la gestión de incidentes.

Auditoría de Acceso y Uso de Datos: Análisis de los registros de acceso a los datos personales para identificar posibles usos indebidos, accesos no autorizados, o violaciones de la política de privacidad. Se deben revisar los permisos de acceso y la correcta aplicación de controles de seguridad.

Informe de Resultados: Elaboración de un informe detallado con los hallazgos de la auditoría, incluyendo recomendaciones para corregir deficiencias y mejorar los procesos de protección de datos. Este informe debe ser revisado por la alta dirección y los responsables de protección de datos.

Monitoreo continuo de la seguridad de los datos.

El monitoreo continuo es esencial para detectar y responder rápidamente a posibles amenazas a la seguridad de los datos personales. Las estrategias de monitoreo deben incluir:

Sistemas de Monitoreo en Tiempo Real: Implementación de herramientas de monitoreo que vigilen continuamente la actividad en los sistemas que almacenan o procesan datos personales. Esto incluye la detección de accesos inusuales, intentos de intrusión, y comportamientos anómalos que podrían indicar una amenaza.

Alertas Automáticas: Configuración de alertas automáticas que notifiquen al equipo de seguridad sobre eventos críticos, como intentos de acceso no autorizado, violaciones de políticas, o actividades sospechosas. Estas alertas deben ser escaladas de acuerdo con la gravedad del incidente.

Registro de Actividades (Logs): Mantener registros detallados de todas las actividades relacionadas con el acceso y manejo de datos personales. Estos registros deben ser revisados regularmente para identificar patrones o tendencias que puedan indicar un riesgo potencial.

Revisión de Controles de Seguridad: Evaluación continua de la efectividad de los controles de seguridad implementados, como firewalls, sistemas de detección de intrusiones, y cifrado de datos. Se deben realizar pruebas periódicas para asegurar que estos controles funcionen correctamente y estén actualizados.

Evaluación de riesgos y vulnerabilidades.

La evaluación regular de riesgos y vulnerabilidades es clave para identificar y mitigar amenazas potenciales a la seguridad de los datos. Este proceso debe incluir:

Evaluaciones de Riesgos Periódicas: Realizar evaluaciones de riesgos de manera regular para identificar nuevas amenazas y evaluar los riesgos existentes. Esto implica revisar las posibles amenazas internas y externas, así como las vulnerabilidades en los sistemas y procesos.

Análisis de Vulnerabilidades: Utilizar herramientas de análisis de vulnerabilidades para escanear los sistemas en busca de fallos de seguridad, configuraciones incorrectas, o software desactualizado. Estos análisis deben ser realizados por profesionales cualificados y pueden complementarse con pruebas de penetración.

Gestión de Riesgos: Desarrollar un plan de gestión de riesgos que priorice las amenazas identificadas y establezca medidas para mitigarlas. Esto incluye la implementación de controles adicionales, la corrección de vulnerabilidades críticas, y la preparación para incidentes que puedan afectar la seguridad de los datos.

Revisión y Actualización de Estrategias: A medida que evolucionan las amenazas y cambian las tecnologías, es fundamental revisar y actualizar las estrategias de gestión de riesgos y vulnerabilidades. El Consejo debe estar preparado para adaptar sus medidas de seguridad a los nuevos desafíos que surjan.

VIII. Gestión de Incidentes

Procedimientos para la gestión de brechas de seguridad en el

El Consejo de la Judicatura debe contar con procedimientos claros y bien definidos para gestionar brechas de seguridad que comprometan datos personales. Estos procedimientos deben incluir:

Detección y Notificación Interna:

Detección Rápida: Establecer sistemas de monitoreo y alertas para la detección inmediata de brechas de seguridad. Todos los empleados deben ser capacitados para identificar posibles incidentes y reportarlos de manera oportuna.

Notificación Interna: Una vez detectada una brecha, debe notificarse de inmediato al equipo de respuesta a incidentes, al responsable de protección de datos y a la alta dirección. La notificación interna debe incluir detalles sobre la naturaleza del incidente, los datos comprometidos, y las posibles causas.

Evaluación Inicial:

Evaluación del Impacto: Realizar una evaluación inicial del alcance y la gravedad de la brecha, identificando los datos afectados, las posibles consecuencias para los titulares de los datos, y el riesgo de daño.

Identificación de la Causa: Determinar la causa raíz de la brecha mediante la revisión de los sistemas afectados, la identificación de vulnerabilidades explotadas, y el análisis de los registros de actividad.

Contención y Erradicación:

Contención Inmediata: Implementar medidas para contener la brecha y evitar su propagación. Esto puede incluir la desconexión de sistemas comprometidos, el bloqueo de accesos no autorizados, o la suspensión de servicios afectados.

Erradicación de la Amenaza: Eliminar la causa de la brecha mediante la reparación de vulnerabilidades, la limpieza de malware o la reconfiguración de sistemas comprometidos. Es crucial asegurar que la amenaza ha sido completamente neutralizada antes de proceder a la recuperación.

Notificación de violaciones de datos a las autoridades competentes.

La notificación de violaciones de datos es una obligación legal y debe realizarse de manera rápida y conforme a la normativa vigente:

Determinación de la Obligación de Notificación:

Evaluación del Umbral de Notificación: Evaluar si la brecha de seguridad requiere notificación a las autoridades competentes, según los criterios legales establecidos (por ejemplo, si la brecha puede resultar en un riesgo significativo para los derechos y libertades de las personas afectadas).

Procedimiento de Notificación:

Notificación a la Autoridad de Protección de Datos: Si se determina que la notificación es necesaria, esta debe realizarse dentro del plazo legal (generalmente 72 horas desde la detección de la brecha). La notificación debe incluir detalles sobre la naturaleza de la brecha, el alcance de los datos comprometidos, las medidas adoptadas, y las posibles consecuencias para los afectados.

Notificación a los Titulares de los Datos: Informar a los individuos afectados sobre la brecha si es probable que esta resulte en un alto riesgo para sus derechos y libertades. La notificación debe ser clara y contener información sobre las medidas que pueden tomar para protegerse, así como las acciones que el Consejo ha tomado para mitigar el impacto.

Mitigación de impactos y medidas correctivas.

Una vez contenida y notificada la brecha, es esencial enfocarse en mitigar los impactos y establecer medidas correctivas para prevenir futuros incidentes:

Mitigación del Impacto:

Soporte a los Afectados: Proporcionar a los titulares de datos afectados el apoyo necesario, como asesoramiento sobre cómo proteger su información personal, ofrecer servicios de monitoreo de crédito si es pertinente, o proporcionar asistencia jurídica.

Revisión y Reparación de Datos: Corregir o reparar los datos personales afectados por la brecha, si es posible, y asegurar que la información esté nuevamente protegida de manera adecuada.

Medidas Correctivas:

Análisis Post-Incidente: Realizar un análisis exhaustivo del incidente para identificar las debilidades en los procesos o sistemas que permitieron la brecha. Este análisis debe conducir a un informe que incluya recomendaciones específicas para evitar incidentes similares en el futuro.

Actualización de Políticas y Procedimientos: Revisar y actualizar las políticas y procedimientos de seguridad a la luz de las lecciones aprendidas. Esto puede incluir mejorar las prácticas de seguridad, actualizar el plan de respuesta a incidentes, o fortalecer la capacitación del personal.

Mejora de la Infraestructura de Seguridad: Implementar mejoras técnicas o de infraestructura que refuercen las defensas del Consejo contra futuras brechas, como la adopción de nuevas tecnologías de seguridad, la renovación de sistemas antiguos, o la mejora de los controles de acceso.

IX. Evaluación y Mejora Continua

Evaluación periódica de la efectividad de las medidas de protección de datos.

Para asegurar que el Consejo de la Judicatura mantiene un alto nivel de protección de datos, es fundamental realizar evaluaciones periódicas de la efectividad de las medidas implementadas:

Revisión Regular de Controles de Seguridad: Realizar auditorías internas y evaluaciones de riesgos de manera regular para verificar que los controles de seguridad implementados siguen siendo efectivos y están en línea con las mejores prácticas. Esto incluye la revisión de políticas de acceso, cifrado, monitoreo de sistemas, y procedimientos de respuesta a incidentes.

Análisis de Incidentes y Brechas de Seguridad: Examinar de forma regular los incidentes de seguridad que hayan ocurrido, incluso aquellos menores, para evaluar la respuesta del Consejo y determinar si las medidas adoptadas fueron adecuadas y efectivas en la protección de los datos personales.

Encuestas y Feedback del Personal: Recoger retroalimentación del personal sobre la implementación de políticas de protección de datos y la efectividad de las capacitaciones recibidas. Este feedback puede proporcionar información valiosa sobre áreas que podrían requerir mayor atención o mejora.

Identificación de áreas de mejora y actualización de políticas y procedimientos.

La identificación continua de áreas de mejora es clave para mantener la relevancia y efectividad de las políticas y procedimientos de protección de datos:

Análisis de Brechas y Desempeño: A partir de las evaluaciones y auditorías realizadas, identificar áreas donde las políticas y procedimientos actuales pueden no ser completamente eficaces o donde existan lagunas que puedan ser explotadas. Esto puede incluir tanto procesos técnicos como organizativos.

Revisión y Actualización de Documentación: Actualizar regularmente las políticas de protección de datos, procedimientos operativos estándar, y guías de mejores prácticas. Esto asegura que todas las documentaciones reflejen las últimas normativas, avances tecnológicos, y lecciones aprendidas.

Implementación de Nuevas Tecnologías: Considerar la adopción de nuevas herramientas y tecnologías que puedan mejorar la protección de datos, como avanzados sistemas de cifrado, mejores soluciones de autenticación, o plataformas de monitoreo más sofisticadas.

Adaptación a cambios en la legislación y avances tecnológicos.

El entorno legal y tecnológico en el ámbito de la protección de datos está en constante evolución, y es crucial que el Consejo de la Judicatura se mantenga actualizado:

Monitoreo de Cambios Legislativos: Establecer un proceso para el monitoreo continuo de cambios en la legislación de protección de datos, tanto a nivel nacional como internacional. Esto asegura que el Consejo pueda adaptar sus políticas y procedimientos para cumplir con nuevas leyes y regulaciones.

Evaluación de Impacto de Cambios Tecnológicos: Evaluar regularmente cómo los avances tecnológicos podrían afectar la protección de datos, tanto positivamente (como nuevas oportunidades para mejorar la seguridad) como negativamente (como nuevas amenazas o vulnerabilidades). Adaptar las estrategias de protección de datos en consecuencia.

Capacitación Continua del Personal: A medida que cambian las leyes y tecnologías, es vital que el personal reciba formación continua para comprender y aplicar correctamente las nuevas políticas y procedimientos. Esto incluye capacitaciones sobre nuevas normativas, uso de nuevas herramientas, y mejores prácticas actualizadas.

Revisión Estratégica Anual: Realizar una revisión estratégica anual de todas las actividades de protección de datos del Consejo, evaluando los logros, identificando áreas de mejora, y estableciendo metas para el siguiente año. Esta revisión debe involucrar a todas las partes interesadas clave, incluyendo la alta dirección, los responsables de protección de datos, y representantes del personal.

X. Conclusiones

Recapitulación de los principales puntos tratados en la guía.

A lo largo de esta guía, hemos abordado los aspectos fundamentales para asegurar la protección de datos personales dentro del Consejo de la Judicatura. Hemos comenzado con una introducción que subraya la importancia de la privacidad en el ámbito judicial, seguido por una revisión detallada del marco legal y normativo que regula esta materia. Además, hemos definido claramente los roles y responsabilidades de los actores involucrados en la protección de datos, y hemos enfatizado la necesidad de formación y concientización constante del personal.

Hemos establecido políticas y procedimientos sólidos para el manejo de datos, discutido las medidas de seguridad técnicas y organizativas necesarias, y delineado los procedimientos para la gestión de incidentes de seguridad. También se ha subrayado la importancia de la auditoría y

el monitoreo continuo para mantener un alto nivel de seguridad. Finalmente, hemos destacado la importancia de la evaluación y mejora continua, asegurando que el Consejo de la Judicatura se mantenga al día con los cambios legales y tecnológicos.

Importancia de la aplicación efectiva de la ley de protección de datos en el Consejo de la Judicatura.

La aplicación efectiva de la Ley de Protección de Datos es fundamental para garantizar la confidencialidad, integridad, y disponibilidad de los datos personales en el ámbito judicial. La protección adecuada de estos datos no solo es una obligación legal, sino también un pilar esencial para mantener la confianza de los ciudadanos en el sistema judicial. Una gestión adecuada de los datos personales refuerza la transparencia, reduce el riesgo de violaciones de datos y sus consecuencias legales, y protege los derechos fundamentales de los individuos.

Compromiso continuo con la privacidad y seguridad de los datos personales.

El Consejo de la Judicatura se compromete a mantener un enfoque proactivo y preventivo en la protección de datos personales. Esto implica no solo cumplir con las normativas vigentes, sino también estar en constante búsqueda de mejoras, adaptando políticas y procedimientos a medida que evolucionan las tecnologías y las amenazas. La privacidad y la seguridad de los datos personales deben estar en el centro de todas las actividades del Consejo, con un compromiso firme de todo el personal en la aplicación de las mejores prácticas y en la promoción de una cultura organizacional que valore y respete la privacidad de los datos.

En resumen, la protección de datos personales no es una tarea puntual, sino un esfuerzo continuo que requiere dedicación, formación, y adaptación constante. El Consejo de la Judicatura reafirma su compromiso con la privacidad y la seguridad de los datos, asegurando que todos los esfuerzos realizados estén orientados a proteger los derechos de los ciudadanos y fortalecer el sistema judicial.

Anexo 2

Validación de la propuesta por los expertos

Especialista 1

Universidad Israel

ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital "Guía para la aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura.". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Edgar Eduardo Ortiz Ganchala
Título obtenido: Doctor en Jurisprudencia y Abogado
C.I.: 1705923009
E-mail: edgar.ortizg@funcionjudicial.com
Institución de Trabajo: Consejo de la Judicatura
Cargo: Subdirector Nacional de Gestión Procesal Penal
Años de experiencia en el área: 32 años

Página 1 de 3

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Guía para la aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	x				
Aplicabilidad	X				
Factibilidad	X				
Novedad	X				
Fundamentación pedagógica	X				
Fundamentación tecnológica	X				
Indicaciones para su uso	X				
TOTAL	35				

Observaciones:

Los derechos no deben ser meramente declarativos, sino que deben atemizar en lo fáctico, y esto a través de protocolos y herramientas tecnológicas, más aún como cuando existe una colisión entre DERECHOS, el uno sobre la transparencia y publicidad de procesos; y, el otro, del de protección de datos personales. Esta tesis aborda con seriedad científica la investigación sobre este espinoso tema, considerando el hecho de que la normativa, al igual que la tecnología son evolutivas, aborda el tema y necesidad de que los datos jurisdiccionales sean temporales. Sugiere con toda lógica llenar el vacío existente entre la Ley de Protección de Datos y la ausencia de un Reglamento que la viabilice, esta investigación ha sido desarrollada de manera seria, y con rigor académico; y, propone la creación de una guía metodológica que limite la publicidad, sin afectarla.

Universidad Israel
ESPOG | Escuela de Posgrados

Existen casos evidentes abordados en el estudio, como el de un ciudadano que ha sido procesado penalmente, y por tanto sus datos son públicos, sin embargo, ésta persona no ha sido declarado culpable de nada, entonces viola el principio de inocencia. Más grave aún resulta para el caso de quien en sentencia ejecutoriada fue objeto de ratificación de su estado de inocencia. Lo que evidentemente afecta su derecho al prestigio, buen nombre; y, reputación.

Con lo dicho esta Guía propuesta, resulta de trascendental importancia, al ser una verdadera necesidad evidente, y permitiría enmendar la lesiva realidad actual de estos casos. En medio de éste impase jurídico, el Consejo de la Judicatura, está en la obligación legal y moral, de hallar una solución, que perfectamente podría ser esta guía de aplicación, para la protección de datos de las personas intervinientes en procesos judiciales. Más aún si consideramos el elemento muy bien traído a colación en la presente investigación, referente a las normas a ser observadas como son las constantes en el bloque de constitucionalidad, Convenios Internacionales; y, lo que en argot jurídico se conoce como Soft Law.

Recomendaciones

Solamente me resta decir que la necesidad histórica, de la existencia de una Guía de Aplicación, tornan en plausible y por demás recomendable, éste tipo de herramientas y protocolos tecnológico, como el propuesto en ésta tesis. Me permito felicitar a la autora de la tesis, y dar un voto de aplauso por su trabajo metódico y fundamental

Lugar, fecha de validación: Quito 30 de agosto del 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Mariscal de Veintimilla, Quito – Ecuador y dirección electrónica de contacto proteccióndatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

Universidad Israel

ESPOG | Escuela de Posgrados

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo proteccióndatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

EDGAR EDUARDO ORTIZ GANCHALA

Firmado digitalmente por EDGAR EDUARDO ORTIZ GANCHALA
Fecha: 2024.08.30 14:36:12 -05'00'

Firma del especialista
Edgar Eduardo Ortiz Ganchala

Especialista 2

Universidad Israel
ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital "Guía para la aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura.". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Iván Javier Cruz Pérez
Título obtenido: Abogado de los Tribunales y Juzgados de la República
C.I.: 180383196-3
E-mail: jcperez_bya@hotmail.com
Institución de Trabajo: Consejo de la Judicatura
Cargo: Analista
Años de experiencia en el área: 3 años

Universidad Israel
ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Guía para la aplicación de la Ley de Protección de Datos en el Consejo de la Judicatura"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	x				
Aplicabilidad	X				
Factibilidad	X				
Novedad		X			
Fundamentación pedagógica	X				
Fundamentación tecnológica	X				
Indicaciones para su uso		X			
TOTAL	25	10			

Observaciones:

El interés público dado la amplitud del término puede dar paso a un tratamiento indebido en datos sensibles y ello conllevar a lesionar derechos inherentes al titular.

Recomendaciones

Limitar el alcance que permite prescindir del consentimiento del titular para el tratamiento de sus datos sensibles con el afán de salvaguardar los derechos que le asisten.

Lugar, fecha de validación: Quito 30 de agosto del 2024

Universidad Israel

ESPOG | Escuela de Posgrados

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto proteccióndatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo proteccióndatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

IVAN JAVIER CRUZ PEREZ

Firma del especialista
Abg. Ivan Javier Cruz Pérez

Especialista 3

Universidad Israel
ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMATICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital "Guía de aplicación para la protección de datos personales de personas intervinientes en procesos judiciales". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Pablo Teodoro Vázquez Cajamarca
Título obtenido: Abogado de los Tribunales de la República del Ecuador
C.I.:0301528022
E-mail: pablo.vazquez@funcionjudicial.gob.ec
Institución de Trabajo: Consejo de la Judicatura
Cargo: Analista 2
Años de experiencia en el área: 9 años

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Guía de aplicación para la protección de datos personales de personas intervinientes en procesos judiciales"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	x				
Aplicabilidad	x				
Factibilidad	x				
Novedad	x				
Fundamentación pedagógica	x				
Fundamentación tecnológica	x				
Indicaciones para su uso	x				
TOTAL	35				

Observaciones

Incorporar la ley en el sistema nacional de registro de datos públicos

Recomendaciones:

DINARP, tiene el objetivo de garantizar la seguridad jurídica, organización, sistematización de registro de datos públicos.

Lugar, fecha de validación: Quito 30 de agosto 2024

Universidad Israel

ESPOG | Escuela de Posgrados

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informatica, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

PABLO TEODORO VAZQUEZ CAJAMARCA

Firmado digitalmente por PABLO TEODORO VAZQUEZ CAJAMARCA
Fecha: 2024.08.30 16:07:33 -05'00'

Firma del especialista
Pablo Teodoro Vázquez Cajamarca

Anexo 3

Encuestas

Encuesta sobre la Protección de Datos Personales en Juzgados y Tribunales

Instrucciones: Por favor, responda las siguientes preguntas basándose en su experiencia y conocimiento en el contexto de su trabajo en el juzgado. Su participación es voluntaria y todas las respuestas serán tratadas con la máxima confidencialidad.

1. Información General

a. ¿En qué área del juzgado trabaja usted? (Especifique su departamento o función)

_ _

b. ¿Cuánto tiempo lleva trabajando en el sistema judicial?

_ _

2. Conocimiento y Formación

a. ¿Ha recibido formación específica sobre protección de datos personales?

- Sí
- No

b. Si la respuesta anterior fue afirmativa, ¿considera que la formación recibida es suficiente?

- Sí
- No

c. ¿Qué áreas cree que deberían reforzarse en la formación sobre protección de datos personales?

_ _
_ _

3. Políticas y Procedimientos

a. ¿Está usted familiarizado con las políticas de protección de datos personales de su juzgado?

- -Sí
- -No

b. En su opinión, ¿son las políticas y procedimientos actuales efectivos para proteger los datos personales?

- Sí
- No

c. ¿Qué aspectos de las políticas y procedimientos actuales considera que necesitan mejoras?

_ _
_ _

4. Prácticas de Manejo de Datos

a. ¿Cómo calificaría la seguridad de los sistemas de manejo de datos personales en su lugar de trabajo?

- Muy segura
- Segura
- Moderadamente segura
- Insegura
- Muy insegura

b. ¿Se utilizan prácticas de anonimización o pseudonimización para proteger los datos personales en los procesos judiciales?

- Siempre
- A menudo
- A veces
- Raramente
- Nunca

c. ¿Existen procedimientos claros para el manejo de brechas de seguridad o violaciones de datos personales?

- Sí
- No

5. Experiencias y Observaciones

a. ¿Ha observado situaciones donde la protección de datos personales pudo haberse comprometido?

- Sí
- No

Si respondió afirmativamente a la pregunta anterior, por favor, describa brevemente la situación y cómo se manejó.

6. Sugerencias y Mejoras

a. Basado en su experiencia, ¿qué cambios o mejoras sugeriría para fortalecer la protección de datos personales en los procesos judiciales?

_____
_____

Gracias por su tiempo y su valiosa contribución a este estudio. Su opinión es crucial para mejorar las prácticas de protección de datos personales en nuestro sistema judicial.