UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
GESTIÓN DE RIESGOS DE DATOS SENSIBLES DE LA DIRECCIÓN GENERAL DE AVIACIÓN CIVIL ALINEADOS AL CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES
Línea de Investigación:
Sistemas de Información e Informática
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor:
Stalin Marcelo Maldonado Almeida
Tutor:
MSc. Pablo Marcel Recalde Varela.

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, MSc. Pablo Marcel Recalde Varela con C.I: 1711685022 en mi calidad de Tutor del proyecto de investigación titulado: "Gestión de riesgos de datos sensibles de la Dirección General de Aviación Civil alineados al cumplimiento de la Ley Orgánica de Protección de Datos Personales".

Elaborado por: Stalin Marcelo Maldonado Almeida, de C.I: 1718528563, estudiante de la Maestría: Seguridad informática, de la UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL), como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

Firma

MSc. Pablo Marcel Recalde Varela
CI. 1711685022

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Stalin Marcelo Maldonado Almeida con C.I: 1718528563, autor del proyecto de titulación denominado: "Gestión de riesgos de datos sensibles de la Dirección General de Aviación Civil alineados al cumplimiento de la Ley Orgánica de Protección de Datos Personales". Previo a la obtención del título de Magister 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., septiembre de 2023

Firmado electrónicamente por:
STALIN MARCELO
MALDONADO ALMEIDA

Firma.
Stalin Marcelo Maldonado Almeida.
CI. 1718528563
ORCID: 0009-0001-6106-3510

Índice de Contenido

Índice de tablas

Índice de figuras

Información General

El crecimiento exponencial de información en línea, sumado a los ataques informáticos cada vez más frecuentes, ha generado la necesidad de creación de leyes que regulen el uso de los datos personales en el país.

Contextualización del Problema.

La gestión de riesgos en la seguridad informática es un proceso crítico, que busca salvaguardar la integridad, confidencialidad y disponibilidad de los sistemas y datos en el ámbito digital. Según Carrillo (2021), en un mundo cada vez más interconectado y dependiente de la tecnología, las amenazas cibernéticas han evolucionado en complejidad y alcance, lo que hace que la gestión de riesgos sea una preocupación central para organizaciones, gobiernos y usuarios individuales por igual.

Según CertiSur (2023), entidad argentina dedicada principalmente a la seguridad electrónica personal y corporativa, en su artículo denominado «La Ciberseguridad IOT en la era del ransomware», el contexto actual del problema en la gestión de riesgos en la seguridad informática incluye varios aspectos clave, entre los más importantes se puede mencionar:

Amenazas Cibernéticas Avanzadas: con el paso de los años e innovación en tecnología, los ciberdelincuentes han desarrollado técnicas cada vez más sofisticadas para infiltrarse en sistemas y redes. Esto incluye malware, ransomware, phishing, ataques de día cero, entre otros métodos de explotación que pueden evadir medidas de seguridad.

Crecimiento del Espacio Digital: La transformación digital conlleva un incremente de procesos y almacenamiento de datos, lo que crea más puntos de entrada potenciales para los atacantes. La proliferación de dispositivos que utilizan Internet de las cosas (IoT) y la interconexión de sistemas incrementa la posibilidad de sufrir un ataque.

Impacto Económico y Reputacional: Los ataques informáticos exitosos pueden tener un alto costo financiero, pero sobre todo en la reputación de las organizaciones. La pérdida de datos confidenciales, la interrupción de servicios y la violación de la privacidad de los clientes pueden resultar en pérdida de confianza y problemas legales.

Regulaciones y Cumplimiento: Las leyes y regulaciones relacionadas con la seguridad informática han tenido un crecimiento en años recientes, lo que obliga a las organizaciones a cumplir con estándares específicos para proteger los datos y la privacidad de los usuarios.

Escasez de Talento Humano especializado en Seguridad Informática: Existe una falta de profesionales capacitados en seguridad informática, lo que dificulta la implementación y mantenimiento efectivo de medidas de seguridad.

Falta de Concienciación: Los usuarios y colaboradores en la mayoría de casos, no están suficientemente informados sobre las buenas prácticas de seguridad informática, lo que crea potenciales vulnerabilidades.

Evolución de la Tecnología: La constante evolución tecnológica introduce nuevas herramientas y enfoques para proteger sistemas, pero también crea nuevos desafíos a medida que los atacantes adaptan sus tácticas.

Dicho esto, la gestión de riesgos en seguridad informática implica identificar, evaluar y mitigar amenazas, las mismas se pueden minimizar mediante la implementación de medidas de seguridad adecuadas, como firewalls de próxima generación, sistemas de detección de intrusiones, encriptación y autenticación de dos factores.

Es así que, la gestión de riesgos es esencial en un mundo digital en constante cambio. Las organizaciones deben adaptarse continuamente a las nuevas amenazas y desafíos, manteniendo una postura proactiva en la protección de sus activos digitales y la mitigación de posibles impactos adversos.

El enfoque de la gestión de riesgos en conjunto con la ley de protección de datos personales se centra en minimizar los problemas relacionados a la seguridad informática y a la privacidad de la información personal recopilada, procesada y almacenada por organizaciones, de manera que se cumplan tanto los requisitos legales como las mejores prácticas de seguridad.

En Ecuador La Ley Orgánica de Protección de Datos Personales (2021) establece los principios, derechos y regulaciones para la protección de la privacidad y la seguridad de los datos personales de los ciudadanos, por ende, se pretende realizar un enfoque de la gestión de riesgos mediante la misma.

Problema Objeto de Investigación.

Con la presente investigación se pretende identificar la data sensible que manejan los sistemas informáticos de la Dirección General de Aviación Civil, ya que, al ser considerada una institución parte del sector estratégico del país, es vital dar el tratamiento pertinente a la data que manejan dichos sistemas de la organización, todo alineado al cumplimiento de la Ley Orgánica de Protección de Datos Personales.

También se busca explorar la efectividad de la gestión de riesgos en el cumplimiento de la Ley Orgánica de Protección de Datos Personales, un análisis de cómo, la Dirección General de Aviación Civil del Ecuador abordaría los problemas de seguridad informática para garantizar la protección de los datos y cumplir con los requisitos legales, con el fin de mitigar los riesgos y sanciones por el incumplimiento de esta ley.

¿Cómo puede la Dirección General de Aviación Civil mitigar problemas relacionados a los datos sensibles de sus sistemas informáticos, para dar cumplimiento a la Ley Orgánica de Protección de Datos Personales?

Objetivo General.

Minimizar problemas relacionados a los datos sensibles de la Dirección General de Aviación Civil, mediante el análisis de riesgo de la data de los sistemas informáticos, en cumplimiento a la Ley Orgánica de Protección de Datos Personales.

Objetivos Específicos.

- Inventariar la data de los sistemas informáticos más representativos de la Dirección General de Aviación Civil.
- Determinar la sensibilidad de los sistemas inventariados, asignando niveles a cada amenaza en función de su probabilidad de ocurrencia y su impacto potencial en los datos personales.
- Identificar los enfoques de riesgo respecto a la información que la organización maneja.
- Sugerir cambios en los enfoques detectados, acorde a la Ley Orgánica de Protección de Datos Personales, además de alinearse al Objetivo de Desarrollo Sostenible 11 establecidos por las Naciones Unidas; que busca contar con ciudades más inclusivas, seguras, resilientes y sostenibles.

Vinculación con la Sociedad y Beneficiarios Directos:

La ciudadanía en general, ya que se pretende garantizar la seguridad operacional de la aviación, proporcionando servicios de calidad para el desarrollo sostenible del transporte aéreo del país.

Beneficiarios Directos.

- La Dirección General de Aviación Civil del Ecuador, ya que con las sugerencias dadas se pretende evitar multas o posibles sanciones y dar cumplimiento a la Ley objeto del presente trabajo de investigación.
- Los trabajadores de la Dirección General de Aviación Civil mediante capacitaciones sobre la gestión de riesgos conjuntamente con la LOPDP.

Beneficiarios Indirectos.

- Empresas privadas nacionales o extranjeras que brinden el servicio de actividades aeronáuticas y aeroportuarias, ya que permitirá minimizar los riesgos con la data que manejen.

Capítulo I: Descripción del Proyecto.

Este proyecto de investigación, busca identificar la data sensible de los sistemas de la DGAC y su tratamiento adecuado, en cumplimiento a los establecido en la LOPDP.

1.1. Contextualización General del Estado del Arte.

A continuación, algunos artículos de sustento para el presente trabajo.

a. Normativa Legal.

a) La Constitución.

La Constitución de Ecuador establece la base para el gobierno y la sociedad en el país. Define cómo se organiza el poder, cómo se eligen los representantes, cuáles son los derechos y responsabilidades de los ciudadanos y cómo funcionan las diferentes instituciones gubernamentales.

La Constitución también puede contener disposiciones específicas relacionadas con la cultura, los valores y las políticas del país, también como la norma suprema que permite que la legislación fundamental se adapte a las cambiantes necesidades y valores de la sociedad. *(Constitución de la República del Ecuador | Registro Oficial 449, 2008)*.

b) Ley Orgánica de Protección de Datos Personales.

Con fecha 10 de mayo de 2021, en la sesión 707, bajo la modalidad virtual, el pleno de la Asamblea Nacional del Ecuador aprobó con 118 votos afirmativos, el proyecto de Ley de Protección de Datos Personales, que fue entregado el pasado 19 de septiembre de 2019 por la Presidencia de la República, a través del Ministerio de Telecomunicación y de la Sociedad de la Información y la Dirección Nacional de Registro de Datos Públicos.

La Ley Orgánica de Protección de Datos Personales es una legislación que tiene como objetivo principal la regulación y protección de datos personales de los ciudadanos, estableciendo los principios y normas que deben seguir las organizaciones publica o privadas y entidades que recopilan, procesan y almacenan información personal.

La Ley Orgánica de Protección de Datos Personales busca garantizar la privacidad, la seguridad y los derechos de las personas en relación con sus datos personales,

mientras que al mismo tiempo permite que las organizaciones puedan utilizar esos datos de manera legítima y responsable.

Algunos de los conceptos más importantes de la LOPDP son:

Principios de Protección de Datos: En donde se establecen los principios básicos que deben regir el procesamiento de datos personales, como la finalidad específica de la recopilación, la minimización de datos, la exactitud, la limitación del almacenamiento y otros.

Consentimiento del Titular de los Datos: Requiere que las organizaciones obtengan el consentimiento informado de los individuos antes de recopilar, procesar o almacenar sus datos personales.

Derechos de los Titulares de Datos: Establece los derechos que tienen los titulares de los datos sobre sus propios datos personales, como el derecho de acceso, rectificación, cancelación y oposición al procesamiento.

Medidas de Seguridad: Obliga a las organizaciones a implementar medidas técnicas y organizativas adecuadas para proteger los datos personales de acceso no autorizado, pérdida, alteración o divulgación.

Transferencia Internacional de Datos: Define las restricciones y requisitos para transferir datos personales a países fuera de la jurisdicción de la ley, asegurando que los datos se mantengan protegidos incluso cuando se transfieran internacionalmente.

Registro de Bases de Datos: Algunas leyes requieren que las organizaciones registren sus bases de datos ante una autoridad de control o entidad reguladora.

Sanciones por Incumplimiento: Establece sanciones y multas en caso de incumplimiento de las disposiciones de la ley, lo que incentiva a las organizaciones a cumplir con las normas de protección de datos.

Autoridades de Control: Designa una autoridad o entidad gubernamental encargada de supervisar el cumplimiento de la ley y de investigar las quejas y violaciones. (*Ley Orgánica de Protección de Datos Personales | Registro Oficial Suplemento No. 459 – 2021*)

b. Riesgo.

De acuerdo a Antonio (2020), el riesgo es la posibilidad de que un evento ocurra y que el mismo tenga un impacto negativo o adverso en un objetivo o resultado deseado,

se puede decir que el riesgo implica la probabilidad de que algo salga mal y cause consecuencias no contempladas.

El concepto de riesgo se aplica en una amplia gama de contextos, desde las finanzas y la inversión hasta la seguridad, la salud, el medio ambiente y muchas otras áreas. Algunos elementos clave relacionados con el riesgo incluyen, la probabilidad, el impacto, la mitigación, la tolerancia al riesgo y el riesgo positivo, mejor conocido como oportunidad.

c. Gestión del Riesgo.

De acuerdo a Carrillo (2021), la gestión de riesgos es un proceso sistemático y continuo que implica identificar, analizar, evaluar y controlar los riesgos que pueden afectar a una organización, proyecto, actividad o cualquier entidad en particular.

El objetivo principal de la gestión de riesgos es minimizar las amenazas y aprovechar las oportunidades para alcanzar los objetivos de manera más eficiente y efectiva. Los pasos a seguir en la gestión de riesgos generalmente son:

Identificación de Riesgos: Es importante, identificar y catalogar todos los riesgos potenciales que podrían afectar los objetivos de la organización.

Análisis de Riesgos: Implica comprender las causas, consecuencias y cómo podría influir en los objetivos.

Evaluación de Riesgos: Permite priorizar los riesgos en función de su importancia y establecer un enfoque adecuado para abordarlos.

Implementación de Medidas de Control: Sirve para gestionar cada riesgo de acuerdo con la estrategia seleccionada, puede incluir cambios en los procesos, asignación de recursos extras y capacitación del personal.

Monitoreo Continuo: Sumamente necesario en función de los cambios en el entorno y la evolución de los riesgos.

Comunicación: Es importante mantener a todas las partes interesadas informadas sobre los riesgos identificados, las estrategias de gestión y los resultados.

La revisión sobre los aspectos más relevantes en cuanto a la gestión del riesgo de la Dirección General de Aviación Civil y la normativa de LOPDP se encuentran detallados en el documento denominado “Comparativa de los riesgos más relevantes, junto a la aplicación de la normativa vigente de LOPDP”; **ver Anexo 1.**

d. Seguridad Informática.

Según Cano (2012), la seguridad informática, se refiere al conjunto de prácticas, medidas y tecnologías diseñadas para proteger los sistemas, las redes, los datos y la información digital contra amenazas, ataques, robos y daños malintencionados.

El objetivo principal de la seguridad informática es garantizar la confidencialidad, la integridad y la disponibilidad de la información en el entorno digital.

Entre los aspectos más importantes de la seguridad informática y que tienen relación con el presente trabajo de investigación se puede mencionar:

Seguridad de Redes: Implementación de firewalls, sistemas de detección de intrusiones y otras medidas para proteger las redes contra ataques y accesos no autorizados.

Cifrado: Uso de técnicas de encriptación para proteger la confidencialidad de los datos mientras se transmiten a través de redes o se almacenan en sistemas.

Gestión de Parches y Actualizaciones: Mantenimiento regular de sistemas y software para corregir vulnerabilidades conocidas y evitar que los atacantes aprovechen brechas de seguridad.

Educación y Concienciación: Capacitar al personal y los usuarios para identificar y prevenir amenazas como el phishing, la ingeniería social y otros ataques basados en la manipulación de la gente.

Respuesta a Incidentes: Tener planes y procedimientos en marcha para detectar, responder y recuperarse de posibles incidentes de seguridad.

Políticas y Normativas: Establecer políticas y normativas internas que definan las prácticas de seguridad, las responsabilidades y los procedimientos para garantizar un enfoque coherente y eficaz.

1.2. Proceso Investigativo Metodológico.

Investigación Cualitativa.

QuestionPro Latinoamérica, entidad proveedora de soluciones para recolección y análisis de datos, paneles de investigación y estudios de clima laboral, en su artículo denominado "Investigación cualitativa" (2022), menciona que es un conjunto de técnicas de investigación que se utilizan para obtener una visión general del comportamiento y la percepción de las personas sobre un tema en particular.

Figura 1.
Tipos de Investigaciones cualitativas más utilizados.

Nota: *Investigación cualitativa | QuestionPro, (2022.)*

En la investigación objeto del presente trabajo se utilizaron varias técnicas como, por ejemplo: entrevistas al personal responsable del manejo de la data, cuestionarios abiertos a empleados de diferentes direcciones elegidos al azar, esto con la intención de tener un panorama más amplio, en cuanto al conocimiento de los procesos que la DGAC tiene para la gestión de riesgos.

El modelo de la encuesta y preguntas se las puede encontrar en el documento denominado "Información de recolección de datos". **Ver Anexo 2.**

De acuerdo la investigación establecida se pudo identificar la percepción que tienen los colaboradores, sobre cómo deben manejar los datos de los usuarios.

De igual manera a través de entrevistas a los funcionarios responsables del manejo de la data, se logró conocer cómo se da la gestión de dichos datos. Finalmente, por medio de los cuestionarios se pudo conocer la calidad en el tratamiento de los datos considerados críticos de la DGAC.

Mediante la entrevista del personal encargado de la data de la organización y con el estudio de los sistemas informáticos de la DGAC, se pudieron obtener los datos plasmados en la Tabla 1.

Tabla 1.
Datos recolectados en las páginas web identificadas de la DGAC.

Portales web - sistemas	Datos que se recolectan
https://www.aviacioncivil.gob.ec/	Comportamiento de navegación en la página, – Datos de ubicación desde donde se accede al sitio (ciudad y país), – Sistema operativo y Navegador utilizado, – Dispositivo que utiliza para acceder al portal. – Datos personales: • Número de cédula de identidad ecuatoriana y o RUC, • Lugar de nacimiento y/o Lugar de Residencia en Ecuador, • Número de documento para extranjeros, • Género, • Nombres y apellidos, • Correo electrónico personal o institucional, • Dirección domiciliaria, • Contacto de emergencia, • Nivel De Estudios • Profesión u ocupación, • Razón social • Nombre: Empresa o Institución • Representante legal, • Dirección de la compañía, • Teléfono de la compañía. – Datos de autenticación: • Nombre de usuario, contraseña (cifrada). • IP desde donde se accede • Fecha y hora de acceso • Fecha de nacimiento • Estado civil

Portales web - sistemas	Datos que se recolectan
https://zimbra.aviacioncivil.gob.ec/	– Comportamiento de navegación en la página, – Datos de ubicación desde donde se accede al sitio (ciudad y país), – Sistema operativo y Navegador utilizado, – Dispositivo que utiliza para acceder al portal. – Datos personales: • Número de cédula de identidad ecuatoriana y o RUC, • Lugar de nacimiento y/o Lugar de Residencia en Ecuador, • Número de documento para extranjeros, • Género, • Nombres y apellidos, • Correo electrónico personal o institucional, • Dirección domiciliaria, • Contacto de emergencia, • Nivel De Estudios • Profesión u ocupación, • Razón social • Nombre: Empresa o Institución • Representante legal, • Dirección de la compañía, • Teléfono de la compañía. – Datos de autenticación: • Nombre de usuario, contraseña (cifrada). • IP desde donde se accede • Fecha y hora de acceso • Fecha de nacimiento • Estado civil

Portales web - sistemas	Datos que se recolectan
https://apps.aviacioncivil.gob.ec/form_vuelos_privados/Login/login	– Comportamiento de navegación en la página, – Datos de ubicación desde donde se accede al sitio (ciudad y país), – Sistema operativo y Navegador utilizado, – Dispositivo que utiliza para acceder al portal. – Datos personales: • Número de cédula de

	identidad ecuatoriana y o RUC, • Lugar de nacimiento y/o Lugar de Residencia en Ecuador, • Número de documento para extranjeros, • Género, • Nombres y apellidos, • Correo electrónico personal o institucional, • Dirección domiciliaria, • Contacto de emergencia, • Nivel De Estudios • Profesión u ocupación, • Razón social – Datos de autenticación: • Nombre de usuario, contraseña (cifrada). • IP desde donde se accede • Fecha y hora de acceso
Portales web - sistemas	Datos que se recolectan
https://www.aviacioncivil.gob.ec/junta-investigadora-de-accidentes-notificacion/	– Comportamiento de navegación en la página, – Ubicación desde donde se accede al sitio (ciudad y país), – Sistema operativo y Navegador utilizado, – Dispositivo que utiliza para acceder al portal. – Datos personales: • Número de cédula de identidad ecuatoriana y o RUC, • Lugar de nacimiento y/o Lugar de Residencia en Ecuador, • Número de documento para extranjeros, • Género, • Nombres y apellidos, • Correo electrónico personal o institucional, • Dirección domiciliaria, • Contacto de emergencia, • Nivel de Estudios • Profesión u ocupación, • Razón social • Nombre: Empresa o Institución • Representante legal, • Dirección de la compañía, • Teléfono de la compañía. – Datos de autenticación: • Nombre de usuario,

	contraseña (cifrada). • IP desde donde se accede • Fecha y hora de acceso • Fecha de nacimiento • Estado civil
Portales web - sistemas	Datos que se recolectan
http://www.boletin.aviacioncivil.gob.ec/	– Comportamiento de navegación en la página, – Datos de ubicación desde donde se accede al sitio (ciudad y país), – Sistema operativo y Navegador utilizado, – Dispositivo que utiliza para acceder al portal. – Datos personales: • Número de cédula de identidad ecuatoriana y o RUC, • Lugar de nacimiento y/o Lugar de Residencia en Ecuador, • Número de documento para extranjeros, • Género, • Nombres y apellidos, • Correo electrónico personal o institucional, • Dirección domiciliaria, • Contacto de emergencia, • Nivel De Estudios • Profesión u ocupación, • Razón social • Nombre: Empresa o Institución • Representante legal, • Dirección de la compañía, • Teléfono de la compañía.

Portales web - sistemas	Datos que se recolectan
Infochanel Grupo institucional de WhatsApp	– Comportamiento de navegación en la página, – Datos de ubicación desde donde se accede al sitio (ciudad y país), – Sistema operativo y Navegador utilizado, – Dispositivo para acceder al portal. – Datos personales: • Número de cédula de identidad ecuatoriana y o RUC, • Lugar de nacimiento y/o Lugar de Residencia en Ecuador, • Número de documento para extranjeros, • Género, • Nombres y apellidos • Correo electrónico personal o institucional, • Dirección domiciliaria, • Contacto de emergencia, • Nivel De Estudios • Profesión u ocupación, • Razón social • Nombre: Empresa o Institución • Representante legal, • Dirección de la compañía, • Teléfono de la compañía. – Datos de autenticación: • Nombre de usuario, contraseña (cifrada). • IP desde donde se accede • Fecha y hora de acceso • Fecha de nacimiento • Estado civil

Nota: *Elaboración propia a partir de entrevista con personal encargado.*

De igual manera, se realizaron entrevistas a los funcionarios responsables de los procesos, en los que se planteó las siguientes interrogantes:

- ¿La DGAC cuenta con un formulario de aprobación para la obtención de datos?
- ¿La DGAC cuenta con acuerdos de confidencialidad de la información recolectada?
- ¿La DGAC cuenta con Políticas de Seguridad de Información dentro TI?
- ¿Al entregar información de la DGAC se los realiza por medios autorizados?
- ¿Se tiene controles de medios electrónicos a utilizar dentro de la institución para salvaguardar la información y evitar fuga de datos?
- ¿El departamento de TI cuenta con controles de acceso a la información de base de datos?

- ¿Si alguna entidad sea pública o privada desea dar por terminado su gestión con la DGAC, se procede a eliminar su información de la base de datos o registros físicos si los tuviera?
- ¿La DGAC cuenta con planes de contingencia en lo que se refiere a la base de datos?
- ¿La DGAC cuenta con personal responsable de seguridad de información y monitoreo de posibles vulnerabilidades dentro de la plataforma?
- ¿La DGAC tiene un responsable del tratamiento de los datos personales?

1.3. Análisis de Resultados.

Como antecedente para el análisis de resultados, es importante conocer que la DGAC tiene la responsabilidad de regular, supervisar y promover la aviación civil en el país, con un enfoque en la seguridad, así como promover el desarrollo sostenible y seguro de la aviación en todas sus formas. Las principales funciones de la DGAC del Ecuador son:

Tabla 2.
Principales funciones de la DGAC.

Función	Descripción
Regulación y Normativas	La DGAC emite regulaciones y normativas relacionadas con la operación, mantenimiento y seguridad de aeronaves, aeropuertos, proveedores de servicios de navegación aérea y otros aspectos de la aviación civil.
Supervisión y Control	La entidad realiza inspecciones y auditorías para asegurarse de que las operaciones aéreas, los aeropuertos y los proveedores de servicios cumplan con las regulaciones y los estándares de seguridad establecidos.
Certificación de Aeronaves y Operadores	La DGAC otorga certificados de aeronavegabilidad a las aeronaves y certificados de explotador de aeronaves a las compañías que cumplen con los requisitos de seguridad y operación.
Gestión de Aeropuertos	La entidad se encarga de la gestión de los aeropuertos en Ecuador, asegurando su operación segura y eficiente.
Control del Tráfico Aéreo	La DGAC supervisa y coordina los servicios de control del tráfico aéreo para garantizar la seguridad y fluidez del tráfico aéreo en el espacio aéreo ecuatoriano.
Investigación de Accidentes e Incidentes Aéreos	La entidad investiga accidentes e incidentes aéreos para determinar sus causas y contribuir a la mejora de la seguridad aérea.
Promoción de la Seguridad Aérea	La DGAC trabaja en conjunto con organismos internacionales y nacionales para promover la cultura de seguridad en la aviación civil, incluyendo la formación y capacitación de profesionales en la industria.
Desarrollo y Planificación	La entidad contribuye al desarrollo y planificación de la infraestructura aeroportuaria y a la modernización de los sistemas de navegación aérea.

Nota: *Elaboración Propia, tomado de varias fuentes de la DGAC.*

Como se puede observar en la información mencionada en la tabla 2, al ser la entidad encargada de regular y supervisar, es importante analizar su operatividad en cuanto a los servicios que brinda para su funcionamiento y verificar el nivel de riesgo.

Es así que se procede a realizar un análisis de las posibles amenazas, escenario y nivel de protección con su respectiva respuesta.

El análisis en cuanto a las funciones principales de la Dirección General de Aviación Civil, más las preguntas realizadas a los funcionarios de dicha entidad, permite tener un panorama en el cual se puede centrar la propuesta de trabajo que permitirá minimizar los riesgos de la data, alineado al cumplimiento de la LOPDP, se obtuvieron los siguientes resultados:

- La DGAC al momento, no cuenta con un formulario de aprobación para la obtención de datos.
- La organización no posee acuerdos de confidencialidad.
- Si bien es cierto, la DGAC cuenta con Políticas de Seguridad de Información dentro TI, las mismas en muchos casos no han sido socializadas con el personal.
- La institución entrega datos por medios autorizados, pero este procedimiento no ha sido revisado periódicamente.
- Al momento no se tienen controles de medios electrónicos, tampoco se tiene herramientas para evitar la fuga de datos.
- El departamento de TICs al momento, si cuenta con controles de acceso a la información de base de datos, sin embargo, en su mayoría no han sido actualizados.
- La DGAC no tiene un procedimiento establecido para la eliminación de información de la base de datos, esto se hace de manera aleatoria.
- Si bien es cierto, la institución cuenta con planes de contingencia en lo que se refiere a la base de datos, los mismos no han sido revisados.
- Al momento la institución no cuenta con personal responsable de seguridad de información, tampoco realiza el monitoreo de vulnerabilidades dentro de sus plataformas.
- La DGAC no ha designado un responsable del tratamiento de los datos personales.

Capítulo II: Propuesta.

La presente propuesta pretende salvaguardar los datos sensibles de los sistemas de la DGAC, mediante el análisis de riesgo de los campos de la data, alineado al cumplimiento de la LOPDP.

2.1. Fundamentos Teóricos Aplicados.

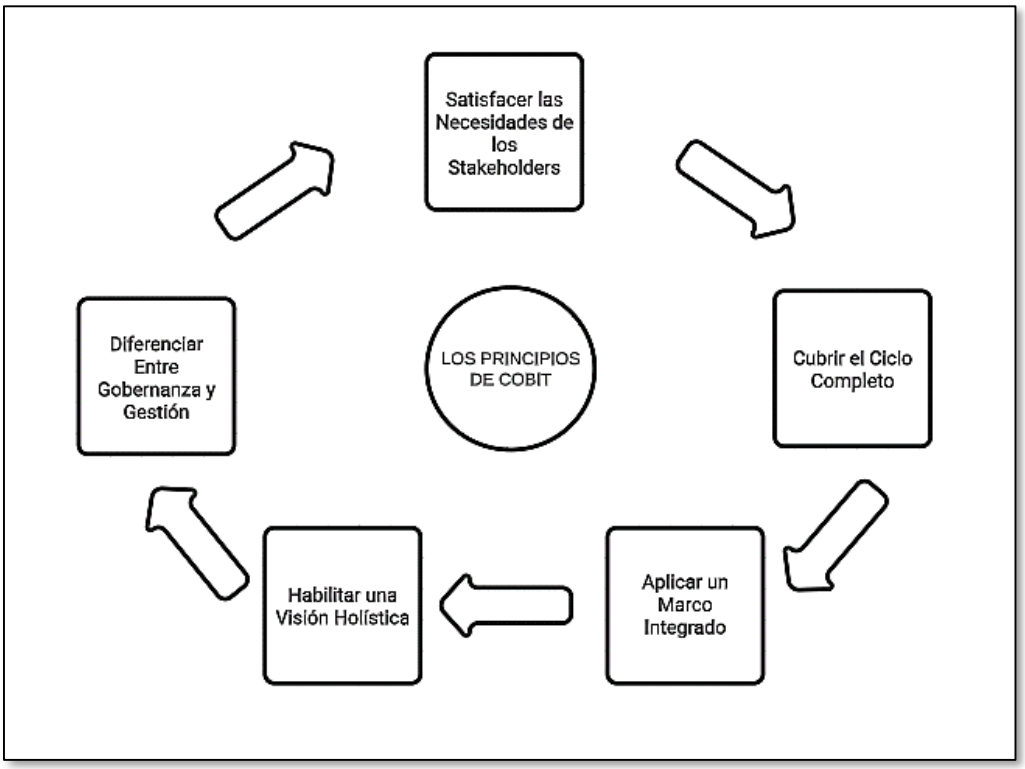
a) COBIT.

Es un marco de referencia desarrollado por Information Systems Audit and Control Association (ISACA) que se enfoca en la gobernanza y gestión de tecnologías de la información (TI) en las organizaciones.

Aunque COBIT tiene un enfoque amplio en la gestión de TI, también se relaciona con la gestión de riesgos, incluida la gestión en el ámbito de la seguridad informática.

De acuerdo a Cortés (2023), COBIT 2019 proporciona un enfoque estructurado para abordar los riesgos relacionados con TI y la seguridad informática, con un marco integral para abordar la gestión de riesgos, ayudando a las organizaciones a establecer procesos efectivos para identificar, evaluar y mitigar los riesgos

Figura 2.
Principios de COBIT.



Nota: *Elaboración propia a partir de COBIT (2019).*

b) Ley Orgánica de Protección de Datos Personales.

La Ley Orgánica de Protección de Datos Personales, pretende salvaguardar los derechos de los ciudadanos en general, otorgando a los titulares, el poder de decisión de a quien entregar su información personal y el tratamiento que se dará a los mismos.

Esta ley consta de 83 artículos, 13 principios que las entidades deben cumplir, además de 14 derechos que buscan proteger a los ciudadanos de la forma en la que se da uso a su información.

«Esta ley transforma no sólo la protección de datos personales, sino también trae cambios drásticos a la industria de la seguridad de la información, por cuanto está basado en la gestión de riesgos» (UASB, 2021).

c) OCTAVE

Por sus siglas "Operationally Critical Threat, Asset, and Vulnerability Evaluation" de acuerdo a Woody (2007) en su artículo "Considering Operational Security Risk during System Development" del Instituto de Ingeniería de Software (SEI), OCTAVE es un enfoque de valoración de riesgos de seguridad de la información diseñado para guiar a las organizaciones a identificar y gestionar los riesgos relacionados con sus activos críticos y procesos operativos.

La metodología OCTAVE por lo general, se lleva a cabo en varias fases:

1. Preparación.
2. Evaluación.
3. Análisis de Riesgos.
4. Planificación de Contramedidas.
5. Implementación.
6. Evaluación de Riesgos Residuales.
7. Integración y Mejora Continua.

2.2. Descripción de la propuesta.

Para alinear la Gestión de Riesgo de la data de la Dirección General de Aviación Civil con la Ley Orgánica de Protección de Datos Personales, se propone como mínimo plantearse las siguientes interrogantes e indicaciones a tomar en cuenta para su manejo.

Interrogantes:

- ¿Qué datos personales se está recopilando?: Es importante comprender y documentar los tipos de datos personales.
- ¿Por qué se está recopilando estos datos?: Es necesario definir el propósito específico de la recopilación.
- ¿Se cuenta con el consentimiento adecuado?: De ser el caso, si se requiere el consentimiento del titular, obtenerlo de manera transparente.
- ¿Cómo se almacenarán y protegerán los datos?: La organización debe evaluar con frecuencia y documentar las medidas de seguridad para evitar accesos no autorizados y posibles pérdidas de datos.
- ¿Quién tendrá acceso a los datos?: Es de suma importancia definir responsables, los mismos serán los que tendrán acceso a los datos bajo ciertas circunstancias.
- ¿Cómo se manejarán las solicitudes de los titulares?: La organización debe establecer procesos para responder a solicitudes de acceso, corrección, eliminación y otros derechos de los titulares de datos.
- ¿Se comparten los datos con terceros?: Si se comparten datos con terceros, es necesario evaluar las prácticas de privacidad y garantizar acuerdos.
- ¿Cómo se eliminarán los datos cuando ya no sean necesarios?: Definir políticas de custodia y procedimientos para eliminar los datos cuando ya no sean requeridos.

Indicaciones:

- Cumplimiento Legal: Asegurarse de cumplir con las leyes de protección de datos y regulaciones vigentes en la normativa.
- Minimización de Datos: Recolectar solo los datos necesarios para el propósito específico y evitar la recopilación excesiva.

- Consentimiento Informado: Obtener el consentimiento explícito e informado de los titulares de datos antes de recopilar y procesar sus datos.
- Transparencia: Proporcionar información clara y comprensible sobre cómo se recopilan, usan y protegen los datos.
- Seguridad de Datos: Implementar medidas técnicas y organizativas adecuadas para proteger los datos contra accesos no autorizados y brechas de seguridad.
- Derechos de los Titulares: Respetar los derechos de los titulares de datos, incluyendo el derecho de acceso, rectificación, eliminación y objeción.
- Evaluación de Riesgos: Realizar evaluaciones de riesgos de privacidad para identificar posibles amenazas y mitigarlas adecuadamente.
- Formación del Personal: Capacitar a los empleados sobre las prácticas de protección de datos y su importancia.
- Políticas y Procedimientos: Establecer políticas internas y procedimientos claros para el manejo de datos personales.
- Auditorías y Revisión Continua: Realizar auditorías regulares y revisar las prácticas de privacidad para asegurarse de que sigan siendo efectivas y se mantengan actualizadas

2.3. Enfoque de riesgo y seguridad.

Con las interrogantes e indicaciones planteadas, es importante establecer el enfoque de riesgo, el enfoque de seguridad, el artículo de la LOPDO que se pretende cubrir y en qué control de COBIT se enmarca dicho enfoque, lo dicho se encuentra resumido en la Tabla 3.

Tabla 3.
Enfoque de riesgo y seguridad.

Gestión de Riesgos	Enfoque Riesgo	Enfoque Seguridad	LOPDP	COBIT 2019
Identificación de Datos Sensibles	La gestión de riesgos implica la identificación de los datos personales que la organización maneja.	Esto incluye identificar qué tipos de datos se están recopilando, cómo se almacenan y procesan, y qué sistemas o procesos están involucrados.	Art. 26	APO12.01
Evaluación de Amenazas y Vulnerabilidades	Una vez que los datos personales se han identificado, se debe evaluar el panorama de amenazas y vulnerabilidades que podrían afectar la seguridad de estos datos.	Incluye analizar las posibles formas en que podrían ser comprometidos por ataques cibernéticos, errores humanos o factores externos.	Art. 40	EDM03.01
Determinación de Riesgos	Basándose en la evaluación de amenazas y vulnerabilidades, se pueden determinar los riesgos específicos para los datos personales.	Esto ayuda a priorizar las medidas de seguridad y decidir cómo mitigar o reducir esos riesgos.	Art. 40	APO12.02
Implementación de Medidas de Seguridad	La gestión de riesgos implica la implementación de medidas de seguridad adecuadas para proteger los datos personales.	Puede incluir: encriptación, controles de acceso, sistemas de detección de intrusiones y capacitación del personal en prácticas seguras.	Art. 38	EDM03.02
Cumplimiento Legal	La ley de protección de datos personales establece requisitos específicos para la recopilación, procesamiento y almacenamiento de datos personales.	La gestión de riesgos debe asegurarse de que las medidas de seguridad implementadas cumplan con estos requisitos legales, incluyendo la notificación adecuada a los titulares de los datos y la obtención de consentimientos.	Art. 12	APO12.01
Planificación de Respuesta a Incidentes	En caso de una brecha de seguridad o violación de datos, la gestión de riesgos debe incluir una planificación de respuesta a incidentes.	Esto implica establecer un plan claro para abordar y comunicar el incidente, minimizar el impacto y cumplir con los requisitos de notificación establecidos por la ley.	Art. 43	DSS04.02
Auditorías y Evaluaciones Continuas	La gestión de riesgos no es un proceso estático. Debe haber una supervisión constante de la efectividad de las medidas de seguridad implementadas.	Esto puede incluir auditorías regulares, pruebas de penetración y evaluaciones de riesgos para asegurarse de que la protección de los datos personales esté actualizada y adaptada a las nuevas amenazas.	Art. 40	DSS04.04

Nota: *Elaboración Propia, basado en fuentes de la DGAC, LOPDP y COBIT.*

Con el enfoque de riesgo y el enfoque de seguridad, plasmado en la Tabla 4, se realizó el análisis referente a los controles de COBIT, la explicación de cada objetivo se encuentra referenciado en las tablas 4, 5 y 6.

Tabla 4.
Objetivos de COBIT 2019 EDM03.

EDM03: Asegurar la optimización del riesgo	
EDM03.01	Evaluar la gestión de riesgos
EDM03.02	Orientar la gestión de riesgos
EDM03.03	Supervisar la gestión de riesgos

Nota: *Elaboración propia a partir de Otake (2019).*

El uso del dominio Evaluar, Dirigir y Monitorear (EDM03) de COBIT denominado "Asegurar la Optimización del Riesgo" es de suma importancia para perfeccionar la gestión de riesgos en todos los aspectos, ya que, de acuerdo a Otake (2019), este dominio proporciona un marco que permite identificar, evaluar, mitigar y monitorear los riesgos, lo que contribuye a la seguridad, eficiencia y cumplimiento normativo.

Tabla 5.
Objetivos de COBIT 2019 APO12.

APO12: Gestionar los riesgos	
APO12.01	Recopilar datos
APO12.02	Analizar el riesgo
APO12.03	Mantener un perfil de riesgo
APO12.04	Riesgo articulado
APO12.05	Definir un portafolio de acciones de gestión de riesgos
APO12.06	Responder al riesgo

Nota: *Elaboración propia a partir de Otake (2019).*

El dominio Alinear, Planificar y Organizar (APO12), denominado "Gestionar los Riesgos", facilita la gestión efectiva de los riesgos relacionados con la amplia gama de funciones y responsabilidades que desempeña la DGAC, el uso de este componente es esencial, ya que, de acuerdo al autor, permite identificar, evaluar y gestionar los riesgos en todas las áreas de influencia de la organización. Esto posibilita proteger los datos sensibles, asegurar operaciones y mantener la continuidad de las mismas.

Tabla 6.
Objetivos de COBIT 2019 DSS04.

DSS04. Gestionar la Continuidad	
DSS04.01	Definir la política de continuidad del negocio, objetivos y alcance
DSS04.02	Mantener una estrategia de continuidad
DSS04.03	Desarrollar e implementar una respuesta a la continuidad del negocio
DSS04.04	Ejercitar, probar y revisar el plan de continuidad
DSS04.05	Revisar, mantener y mejorar el plan de continuidad
DSS04.06	Proporcionar formación en el plan de continuidad
DSS04.07	Gestionar acuerdos de respaldo

Nota: ***Elaboración*** *propia a partir de Otake (2019).*

El dominio Entregar, Dar Soporte y Servir (DSS04), denominado "Gestionar la Continuidad" es esencial para la DGAC, tanto para la continuidad operativa, como para la protección de los datos sensibles que maneja. Dado el alcance y las funciones de la DGAC, este dominio permite minimizar los riesgos sobre dicha data incluso en situaciones de emergencia o desastres.

De los artículos establecidos en la LOPDP se tomarán los más críticos en cuanto a la gestión de riesgos establecida en la DGAC, con el fin de alinear y verificar si existe o no el cumplimiento a la ley vigente y de ser el caso proponer una alineación a la misma.

En la tabla 8, se puede observar los artículos de la LOPDP más relevantes que fueron tomados en consideración, para el presente proyecto de investigación.

Tabla 7.
Artículos de la Ley Orgánica de Datos Personales.

Ley Organica de Protección de Datos Personales	
Artículo	Ley
Art. 12	Derecho a la información
Art. 13	Derecho de acceso
Art. 17	Derecho a la portabilidad
Art. 26	Tratamiento de datos sensibles
Art. 33	Transferencia o comunicación de datos personales
Art. 35	Acceso a datos personales por parte de terceros
Art. 38	Medidas de seguridad en el ámbito del sector público
Art. 40	Análisis de riesgo, amenazas y vulnerabilidades
Art. 43	Notificación de vulneración de seguridad

Nota: *Elaboración propia a partir de la LOPDP (Gob.ec (2021)).*

Como se puede observar, la LOPDP instaura varios artículos que se deben tomar en cuenta para la gestión y manipulación de datos personales, para el objeto del presente trabajo, se tomaron en cuenta los que más se apegan a las necesidades de la organización, a su vez con el marco de referencia de COBIT se puede sugerir la implementación de buenas prácticas en cuanto a los objetivos de gobierno y gestión, para minimizar los riesgos de la data.

1. Formulario de Aprobación: La organización debe proporcionar información clara, sobre cómo se utilizarán dichos datos y permitir que los usuarios acepten o no el uso de los mismos.
2. Reducción de Datos**:** La DGAC debe recolectar única y exclusivamente los datos necesarios para cumplir el propósito específico para el cual se recolectan.
3. Seguridad de los Datos: Por ejemplo, utilizar métodos de cifrado en los datos sensibles y mantener sistemas de seguridad debidamente actualizados, además de establecer niveles de control de acceso para limitar quiénes pueden usar dichos datos.
4. Derechos de los Titulares: Dar a conocer los derechos en relación a los datos personales, por ejemplo: derecho de acceso, enmienda, eliminación y oposición. De igual manera, establecer procedimientos para que los usuarios puedan ejercer sus derechos.
5. Políticas de Conservación: Esto implica almacenar los datos únicamente durante el tiempo necesario para cumplir el propósito original.
6. Capacitación y Concienciación: Capacitar a los funcionarios sobre la importancia de la protección de datos y la privacidad de los mismos, y cómo manejar los datos de manera segura.
7. Auditorías: La organización debe realizar auditorías periódicas, tanto internas como externas, esto permite evaluar la efectividad de las medidas de seguridad.
8. Gestión de Incidentes: La DGAC requiere establecer un plan de respuesta a incidentes o violación de los datos. Es vital, definir procedimientos para notificar a las autoridades y a los eventuales afectados en caso de requerirse.
9. Política de Privacidad: La organización tiene la obligación de explicar de manera clara y concisa, el método mediante el cual se recopilan, utilizan y protegen los datos de los usuarios. Proporcionando de igual manera detalles sobre sus derechos.

Con la implementación de estas medidas, es posible minimizar los problemas relacionados al uso de los datos personales recopilados, además permite alinearse al

cumplimiento de la LOPDP, brindando al usuario final, la confianza de que sus datos están siendo tratados de manera segura.

Conforme a la información recopilada sobre los sistemas informáticos de la DGAC, mediante la entrevista realizada al personal encargado y el análisis de dichos sistemas, tomando como base la metodología OCTAVE se procedió a realizar un análisis de sensibilidad, a partir de la clasificación en función de las amenazas y probabilidad de ocurrencia, bajo el criterio plasmado en la Tabla 8.

Tabla 8.
Análisis de sensibilidad, basado en OCTAVE.

Análisis de sensibilidad			
	Probabilidad Alta	Probabilidad Media	Probabilidad Media
Impacto Alto	Sensibilidad Alta	Sensibilidad Media	Sensibilidad Baja
Impacto Medio	Sensibilidad Media	Sensibilidad Media	Sensibilidad Baja
Impacto Bajo	Sensibilidad Baja	Sensibilidad Baja	Sensibilidad Baja

Nota: *Elaboración propia, a partir de OCTAVE.*

En la matriz de la tabla 8, la probabilidad representa que una amenaza específica se concrete y dicha amenaza afecte al sistema, el impacto como su nombre lo indica, es el impacto a los datos si la amenaza se efectúa, por otro lado, la sensibilidad evalúa el nivel de sensibilidad en función al impacto y a la probabilidad.

Para el presente proyecto, se identificó las potenciales amenazas que podrían afectar a los sistemas, también se evaluó la probabilidad de ocurrencia de las amenazas, además del impacto que dicha amenaza tendría en la protección de los datos.

Se obtuvieron los resultados plasmados en la tabla 9.

Tabla 9.
Sensibilidad Plataformas WEB – DGAC.

Plataformas WEB	Sensibilidad
https://www.aviacioncivil.gob.ec/	Alta
https://zimbra.aviacioncivil.gob.ec/	Alta
https://apps.aviacioncivil.gob.ec/form_sobrevuelos/Login/login	Media
https://apps.aviacioncivil.gob.ec/form_vuelos_privados/Login/login	Media
https://www.aviacioncivil.gob.ec/junta-investigadora-de-accidentes-notificacion/	Alta
http://www.boletin.aviacioncivil.gob.ec/	Baja
http://www.nssp.aviacioncivil.gob.ec/Formularios/reporte_voluntario_ATS.aspx	Media
http://www.nssp.aviacioncivil.gob.ec/Formularios/reporte_accidentes_incidentes_RIPO.aspx	Media

http://www.nssp.aviacioncivil.gob.ec/Formularios/reporte_sucesos_ATS.aspx	Media
http://www.nssp.aviacioncivil.gob.ec/Formularios/reporte_impacto_aviario_IBIS.aspx	Media
http://www.nssp.aviacioncivil.gob.ec/Formularios/reporte_aero.aspx	Media

Nota: *Elaboración Propia, tomado de varias fuentes de la DGAC*.

En la actualidad los datos personales son de acceso público, motivo por el cual, cualquier persona, puede acceder a esta información en la medida esta se encuentre publicada.

Tabla 10.
Acciones en sistemas con sensibilidad alta.

Sistemas con Sensibilidad Alta:	
Encriptación Fuerte:	Utilizar la encriptación de extremo a extremo para proteger los datos sensibles en tránsito y en reposo.
Acceso Controlado:	Limitar el acceso a usuarios autorizados y emplear autenticación de múltiples factores para aumentar la seguridad de las cuentas.
Auditoría y Monitoreo Continuo:	Implementar sistemas de auditoría y monitoreo en tiempo real para detectar actividades inusuales o sospechosas.
Gestión de Vulnerabilidades:	Realizar análisis de vulnerabilidades y parches de forma proactiva para evitar amenazas conocidas.
Respuesta a Incidentes:	Establecer un plan de respuesta a incidentes detallado para actuar rápidamente en caso de una violación de seguridad.

Nota: *Elaboración Propia, a partir de OCTAVE.*

Algo que también se pudo evidenciar, es que, los servidores que realizan el tratamiento de datos personales, no han suscrito acuerdos de confidencialidad. En base al análisis realizado, se recomienda tomar las acciones descritas en las tablas 10, 11 y 12.

Tabla 11.
Acciones en sistemas con sensibilidad media.

Sistemas con Sensibilidad Media:	
Políticas de Acceso:	Implementar políticas sólidas de gestión de acceso para asegurar que solo usuarios autorizados tengan acceso.
Seguridad de la Red:	Utilizar firewalls y soluciones de seguridad de red para protección contra amenazas externas.
Copias de Seguridad Regulares:	Realizar copias de seguridad de datos críticos y almacenarlas en ubicaciones seguras y separadas.
Actualizaciones de Software:	Mantener el software actualizado para protección contra vulnerabilidades conocidas.
Concientización de los Empleados:	Capacita a los empleados sobre prácticas seguras de manejo de datos y cómo reconocer amenazas de seguridad.

Nota: *Elaboración Propia, a partir de OCTAVE.*

Con las medidas descritas en las tablas 10, 11 y 12, se puede minimizar el riesgo sobre los datos de la DGAC.

Tabla 12.
Acciones en sistemas con sensibilidad baja.

Sistemas con Sensibilidad Baja:	
Seguridad Básica:	Se recomienda aplicar medidas básicas de seguridad, como contraseñas fuertes y actualizaciones de software.
Auditoría Periódica:	Realizar auditorías periódicas que aseguren el cumplimiento de políticas de seguridad.
Copias de Seguridad Regular:	Aunque la sensibilidad es baja, se recomienda realizar copias de seguridad de los datos importantes.
Restricción de Acceso:	Limitar el acceso a datos solo a quienes lo necesitan y asegurarse que los archivos sean accesibles solo para usuarios autorizados.
Concientización de los Empleados:	Incluso para sistemas con sensibilidad baja, es importante que los empleados estén conscientes de las prácticas de seguridad.

Nota: *Elaboración Propia, a partir de OCTAVE.*

Es importante tomar en cuenta que la protección de datos es un esfuerzo constante, para que el mismo funcione es necesario, evaluar y ajustar las medidas de seguridad en base a los cambios y necesidades de la organización.

En lo que a los enfoques de riesgo refiere, se acuerdo a los datos obtenidos de la entrevista plasmada en el capítulo 1, tomando como base la metodología OCTAVE se procedió a realizar un análisis de prioridad de riesgos, a partir de la clasificación según su impacto y probabilidad, bajo el criterio plasmado en la Tabla 13.

Tabla 13.
Análisis de prioridad, basado en OCTAVE.

Análisis de prioridad				
	Impacto Alto	Impacto Medio	Impacto Bajo	Impacto Insignificante
Probabilidad Alta	Riesgo Critico	Riesgo Importante	Riesgo Moderado	Riesgo Menor
Probabilidad Media	Riesgo Importante	Riesgo Moderado	Riesgo Menor	Riesgo Aceptable
Probabilidad Baja	Riesgo Moderado	Riesgo Menor	Riesgo Aceptable	Riesgo Aceptable
Probabilidad Muy Baja	Riesgo Menor	Riesgo Aceptable	Riesgo Aceptable	Riesgo Aceptable

Nota: *Elaboración propia, a partir de OCTAVE.*

En la matriz de la tabla 13, se tomaron en cuenta los siguientes criterios:

- Impacto alto, medio, bajo o insignificante: Se tomó como parámetro la gravedad o consecuencia que tendría la ejecución del riesgo en relación con los datos protegidos.

- Probabilidad alta, media, baja o muy baja: Determinado por la posibilidad de ocurrencia del riesgo determinado previamente a través de la entrevista.
- Riesgo Crítico, importante, moderado menor o aceptable: Esta clasificación se da en función del impacto y la probabilidad.

Figura 3

Impacto del enfoque.

Enfoque	Impacto				Justificación
	Alto	Medio	Bajo	Insignificante	
¿La DGAC cuenta con un formulario de aprobación para la obtención de datos?	X				No contar con el formulario requerido tiene un impacto muy importante.
¿La DGAC cuentan con acuerdos de confidencialidad de la información recolectada?	X				La organización no dispone de acuerdos de confidencialidad, por lo que el impacto es alto.
¿La DGAC cuenta con Políticas de Seguridad de Información dentro TI?		X			La DGAC cuenta con politicas, sin embargo no han sido actualizadas, esto no tiene un impacto tan importante.
¿Al entregar información de la DGAC se los realiza por medios autorizados?		X			Si lo hace, sin embargo se debe reforzar el proceso, impacto medio.
¿Se tiene controles de medios electrónicos a utilizar dentro de la institución para salvaguardar la información y evitar fuga de datos?		X			No contar con los controles requeridos, tiene un impacto importante.
¿El departamento de TI cuenta con controles de acceso a la información de base de datos?			X		Si dispone, y estan actualizados, por lo que el impacto es bajo.
¿Si alguna entidad desea dar por terminado su gestión con la DGAC, se procede a eliminar su información de la base de datos?	X				No se tiene politicas al respecto, el impacto es significativo.
¿La DGAC cuenta con planes de contingencia en lo que se refiere a la base de datos?		X			Si, dispone por lo que el impacto no es critico.
¿La DGAC cuenta con personal responsable de seguridad de información y monitoreo de posibles vulnerabilidades?		X			Si bien no dispone de personal especializado, esto puede ser planificado.
¿La DGAC tiene un responsable del tratamiento de los datos personales?	X				No dispone y nadie se hace cargo, por lo que el impacto es elevado.

Nota: *Elaboración propia a partir del enfoque de gestión de riesgo de la DGAC.*

En base al análisis y al criterio de los expertos entrevistados, se obtuvo la matriz resumida en la Tabla 14, con la situación actual de la organización, la misma que permite proponer una aplicación o mejora con la LOPDP y el marco de referencia COBIT, este análisis se puede encontrar a detalle en el documento denominado "Análisis de riesgos". **ver Anexo 5.**

Tabla 14.
Análisis de riesgo situación actual.

Enfoque	Estado actual	Propuesta	Prioridad
¿La DGAC cuenta con un formulario de aprobación para la obtención de datos?	NO	Establecer el "Formulario de Aprobación" de acuerdo a las necesidades.	Crítico
¿La DGAC cuentan con acuerdos de confidencialidad de la información recolectada?	NO	Establecer "Acuerdos de Confidencialidad" para los encargados de manejar los datos.	Crítico
¿La DGAC cuenta con Políticas de Seguridad de Información dentro TI?	SI	Socializar y reforzar dichas políticas.	Importante
¿Al entregar información de la DGAC se los realiza por medios autorizados?	SI	Mejorar el control	Importante
¿Se tiene controles de medios electrónicos a utilizar dentro de la institución para salvaguardar la información y evitar fuga de datos?	NO	Contar con Controles de Seguridad	Importante
¿El departamento de TI cuenta con controles de acceso a la información de base de datos?	SI	Auditar periódicamente los accesos realizados.	Aceptable
¿Si alguna entidad desea dar por terminado su gestión con la DGAC, se procede a eliminar su información de la base de datos?	NO	Establecer "Políticas de Conservación" con procesos y tiempos claros.	Crítico
¿La DGAC cuenta con planes de contingencia en lo que se refiere a la base de datos?	SI	Sugerir mejoras de acuerdo a la LOPDP	Importante
¿La DGAC cuenta con personal responsable de seguridad de información y monitoreo de posibles vulnerabilidades dentro de la plataforma?	NO	Establecer profesionales especializados en Seguridad Informática.	Importante
¿La DGAC tiene un responsable del tratamiento de los datos personales?	NO	Establecer un responsable	Crítico

Nota: *Elaboración propia a partir del enfoque de gestión de riesgo de la DGAC.*

Una vez identificado el enfoque y con propuesta sugerida, se procedió a realizar un análisis de brecha de cada enfoque, para determinar su prioridad, se esto se efectuó un análisis de riesgos y probabilidades, mediante el cual se evalúo las consecuencias y la probabilidad de

que un problema pueda ocurrir si el mismo no se aborda. Esto permite seleccionar las áreas que podrían causar mayores problemas, dicho análisis de brecha y su alineación a COBIT y a la LOPDP, se encuentra resumido en la Tabla 15.

Tabla 15.
Análisis de brecha alineada a la LOPDP y marco de referencia COBIT 2019.

Enfoque	Estado actual	Realizar bajo la LOPDP	COBIT 2019
¿ La DGAC cuenta con un formulario de aprobación para la obtención de datos?	NO	Realizar bajo el Art. 38 de la LOPDP	APO14
¿La DGAC cuentan con acuerdos de confidencialidad de la información recolectada?	NO	Realizar bajo el Art. 8 de la LOPDP	APO13
¿La DGAC cuenta con Políticas de Seguridad de Información dentro TI?	SI	Realizar bajo el Art.37 de la LOPDP	APO13
¿Al entregar información de la DGAC se los realiza por medios autorizados?	SI	Realizar bajo el Art. 17 de la LOPDP	APO14
¿Se tiene controles de medios electrónicos a utilizar dentro de la institución para salvaguardar la información y evitar fuga de datos?	NO	Realizar bajo el Art. 17 de la LOPDP	APO14
¿El departamento de TI cuenta con controles de acceso a la información de base de datos?	SI	Realizar bajo el Art.37 de la LOPDP	APO13
¿Si alguna entidad desea dar por terminado su gestión con la DGAC, se procede a eliminar su información de la base de datos?	NO	Realizar bajo el Art. 15 de la LOPDP	APO14
¿La DGAC cuenta con planes de contingencia en lo que se refiere a la base de datos?	SI	Realizar bajo el Art. 40 de la LOPDP	APO12
¿La DGAC cuenta con personal responsable de seguridad de información y monitoreo de posibles vulnerabilidades dentro de la plataforma?	NO	Realizar bajo el Art. 43 de la LOPDP	MEA02
¿La DGAC tiene un responsable del tratamiento de los datos personales?	NO	Establecer responsables de acuerdo al Art. 48 de la LOPDP	APO14

Nota: *Elaboración propia a partir del enfoque de gestión de riesgo de la DGAC.*

La matriz plasmada en la Tabla 15, fue entregada como propuesta a la Dirección de TICs, para su evaluación, ejecución y puesta en marcha con la finalidad que la gestión de riesgo de los datos sensibles que maneja la DGAC se encuentre alineada a la LOPDP.

Como se puede observar la propuesta entregada, contempla temas referentes a la Ley y al marco de buenas prácticas COBIT, adicionalmente, de la presente investigación, se desprende el siguiente análisis:

Referente a las Políticas de Seguridad de Información y Privacidad (APO14): Se logró identificar la falta de formularios de aprobación al momento de recolectar información, ausencia de acuerdos de confidencialidad y nula eficiencia en la eliminación de información cuando finaliza alguna gestión especifica. Por lo que, es de suma importancia, que la DGAC, desarrolle e implemente procedimientos, con la finalidad de brindar la protección adecuada de los datos y a su vez cumplir con los requisitos de la LOPDP, sobretodo lo establecido en el artículo 38, que refiere a las "Medidas de seguridad en el ámbito del sector público".

Respecto a los Controles de Acceso y Medios Electrónicos (APO13 y APO14): La DGAC requiere fortalecer los controles de acceso e instaurar controles de medios electrónicos para prevenir fugas de datos, por ejemplo, con la implementación de una herramienta "Data Loss Prevention" (DLP), que sirve para evitar que los usuarios envíen información crítica fuera de la red institucional. Estos esfuerzos están alineados con las recomendaciones de COBIT 2019 y también se relacionan con los requisitos legales de la LOPDP, énfasis especial en el artículo 8 "Consentimiento" y el artículo 37 "Seguridad de datos personales".

Respecto a los planes de contingencia (APO12), aunque la DGAC cuenta con estos planes, en lo que se refiere a la base de datos, se sugiere mejorarlos de acuerdo a nuevas tecnologías y de acuerdo a lo descrito en el artículo 40 de la LOPDP "Análisis de riesgo, amenazas y vulnerabilidades". Esta mejora se alinea con las prácticas recomendadas por COBIT y permite brindar una respuesta adecuada en caso de incidentes.

Algo de suma importancia, es el Talento Humano, en este caso, profesionales de Seguridad Informática, se identificó la necesidad de contar con profesionales en este rubro. De acuerdo al dominio "Monitorear, Evaluar y Evaluar el Rendimiento" (MEA02) de COBIT, esto es transcendental para monitorear vulnerabilidades y garantizar la seguridad de las diferentes plataformas y los datos que contienen las mismas. Esta acción se alinea a lo descrito en el artículo 43, "Notificación de vulneración de seguridad" de la LOPDP.

La DGAC demanda contar con un responsable de tratamiento de datos, tomando como referencia lo establecido en el dominio “Alinear, Planificar y Organizar” (APO14), y a lo requerido en el artículo 48 denominado “Delegado de protección de datos personales”.

a. Explicación del aporte.

El aporte del presente consiste en que a partir del mismo se puede minimizar los riesgos a los que se encuentra expuestos los datos de la DGAC, eso implica proteger a la ciudadanía en general, ya que mediante el cumplimiento de la ley se puede preservar la privacidad y evitar que los datos sean utilizados de manera inapropiada.

Con las sugerencias dadas a la organización, la confianza de los usuarios crece exponencialmente, ya que las entidades que cumplen con la ley demuestran su compromiso con la privacidad y la seguridad de los datos de sus usuarios, esto es fundamental para fortalecer la imagen institucional y la reputación de la DGAC y así evitar tener multas y sanciones legales.

Adicionalmente y de acuerdo a Moran (2020), en su publicación **“**El Objetivo de Desarrollo Sostenible”, el ODS 11 tiene como objetivo "lograr que las ciudades y los asentamientos humanos sean inclusivos, seguros, resilientes y sostenibles", al incluir las sugerencias dadas en la organización, la misma está preparada para enfrentar los riesgos de sus datos ante desastres naturales, esto gracias a los planes de contingencia, con esto se pretende contribuir a la consecución del objetivo 11, esto se resume en las Tablas 16 y 17.

Tabla 16.
Aporte al ODS N°11 en la DGAC.

Gestión de Riesgos	
Resiliencia de Ciudades y Asentamientos	Mediante la evaluación de riesgos y la implementación de medidas de mitigación, la infraestructura de la DGAC puede estar preparadas para enfrentar desastres naturales, minimizar daños y recuperarse más rápidamente y poder brindar una continuidad del servicio.
Planificación Urbana Sostenible	Es importante la identificación de zonas de riesgo y la adopción de regulaciones para futuras construcción en caunto a operaciones y esto pueden reducir la vulnerabilidad de las áreas urbanas, promoviendo la seguridad de la población y la infraestructura para la DGAC

Nota: *Elaboración propia a partir los ODS.*

Es elemental tener en claro las zonas de riesgo donde se encuentran las instalaciones que manejan la data, si no se tiene claro los peligros de la zona, no se puede gestionar adecuadamente el riesgo.

Tabla 17.
LOPDP aporte al ODS N°11 en la DGAC.

Ley Orgánica de Protección de Datos Personales	
Privacidad y Seguridad de los Residentes	La protección de datos personales garantiza que los datos de los ciudadanos, incluyendo información sensible, estén resguardados y no sean utilizados de manera indebida
Transparencia y Confianza	Al establecer reglas claras para la recopilación, el almacenamiento y el uso de datos, se genera confianza en las instituciones y organizaciones que operan en las ciudades y asentamientos.

Nota: *Elaboración propia a partir los ODS.*

Con el cumplimiento de la LOPDP se incide directamente en el ámbito de "Privacidad y seguridad de los residentes", que es uno de los objetivos de desarrollo sostenible 11.
Cabe recalcar que esta propuesta es solo una sugerencia y que los controles pueden variar según las necesidades y requisitos de la organización, en este caso de la DGAC.

b. Estrategias y técnicas.

Para el desarrollo de esta investigación, se procedió con el análisis y revisión de la ley orgánica de protección de datos personales, así como también el marco de referencia de buenas prácticas de COBIT, los mismos que permitieron desarrollar el eje de la propuesta.

Se realizó un análisis de brechas de la situación actual de la data de la DGAC para poder saber desde donde se puede partir y hasta donde se va a llegar con la propuesta del producto.

En resumen, la estrategia fue tomar como base los artículos de la LOPDP y el marco de referencia COBIT, con el fin de sugerir controles, políticas y demás tratamiento necesario, con la finalidad de cumplir con la ley y a su vez implementar buenas prácticas, todo de acuerdo a la gestión de riesgos de la DGAC.

2.3. Valoración de la propuesta.

La propuesta del presente trabajo, ha sido revisada por tres expertos de diferentes áreas de tecnología, incluido el Oficial de Seguridad de la DGAC, teniendo como resultado, que el documento ofrece una guía consistente, que permite sentar las bases para abordar el cumplimiento de la Ley Orgánica de Protección de Datos Personales y tener un enfoque que sirve de referencia para alinear los procesos a los dominios de COBIT.

Tomando en cuenta las sugerencias plasmadas, el presente trabajo se convierte en una herramienta efectiva para que la DGAC o cualquier entidad de similar organización que busque una guía para proteger sus datos pueda hacer uso del mismo.

El criterio otorgado por los expertos, resalta el valor de la propuesta. Su alineación a la ley y a estándares reconocidos, el enfoque dado y la capacidad de adaptarse a las nuevas tendencias, convierten a este trabajo una guía básica en la búsqueda de seguridad y protección de datos sensibles dentro de una organización

En resumen, los expertos manifiestan que la propuesta, implica una serie de acciones necesarias para fortalecer la seguridad de la información y la asegurar los datos de la DGAC. Dichas acciones no solo permitirán cumplir con los requisitos legales establecidos por la LOPDP, sino que también se alinean con las mejores prácticas recomendadas por COBIT y que al implementar estas acciones se gestionará de manera efectiva los riesgos relacionados con la seguridad de los datos y se asegurará el cumplimiento de la ley.

2.4. 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.

Tabla18.
Matriz de articulación.

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Investigación de la ley vigente (LOPDP)	Ley Orgánica de Protección de Datos Personales	Revisión documental y experimental	Revisión de la Ley vigente	De acuerdo a la revisión se puede verificar ciertos artículos que ayudaran a cumplir con lo establecido en la normativa vigente	Documentos de archivo y fuentes gubernamentales
Estudio al marco de referencia COBIT 2019	Marco de referencia para Gobierno y Gestión de TI	Revisión documental y experimental	Revisión de la actualización vigente	Manejo de buenas prácticas para la implementación de objetivos de gobierno y gestión	Documentos de archivo y fuentes gubernamentales
Encuestas a grupos focales y entrevistas a funcionarios	Proceso de investigación cualitativa	Encuestas, revisión documental, entrevistas.	Elaboración de encuestas y entrevistas	Se desarrolla encuestas y entrevistas con el fin de conocer la situación actual de la DGAC.	Encuestas, entrevistas
Análisis de brechas	Análisis de riesgos y probabilidades	Experimental	Elaboración de matriz	El análisis de brecha ayuda a identificar en qué punto se encuentra la institución en cuanto al tratamientos de datos y a qué punto se quiere llegar.	Investigación / Observaciones

Fuente: Elaboración propia a partir de varias fuentes.

CONCLUSIONES

Mediante el proceso de inventario de los sistemas informáticos se obtuvo una visión clara y completa de cómo los datos personales fluyen a través de la DGAC, lo que a su vez permite implementar medidas efectivas para salvaguardar la integridad y confidencialidad de esta información sensible, ya que la identificación de los puntos de entrada y recopilación de datos personales.

La organización maneja de manera displicente los datos de sus sistemas, lo que ocasiona en muchos casos que estos sean utilizados de mala manera, produciendo inclusive, perdida de los mismos.

Mediante la calificación de los riesgos en la matriz se logró determinar la sensibilidad de los datos y si los mismos cumplen con un enfoque acorde a la LOPDP o si los mismos se alinean a las buenas prácticas del marco de referencia COBIT con el fin de prevenir incidentes durante el tratamiento de dichos datos.

Con la identificación de los enfoques de riesgo de la información que maneja la organización, se puede tener un panorama de las medidas a tomar, de igual manera con la revisión y análisis de la normativa vigente de la Ley Orgánica de Protección de Datos Personales, y en relación con el marco de referencia COBIT 2019, se pudo sugerir los cambios necesarios y determinar la importancia de la gestión de riesgos en el ámbito de la protección de datos.

Al ser los ciudadanos a nivel nacional los beneficiarios directos de esta propuesta en cuanto al manejo y tratamiento de los datos de pudo identificar que se aporta con el Objetivo de Desarrollo Sostenible 11, ya que se establece al derecho de la protección de los datos en las comunidades.

RECOMENDACIONES

Implementar medidas eficientes que permitan minimizar el riesgo de los datos, a su vez establecido el marco de trabajo de la gestión de riesgos aplicando la LOPDP y COBIT se recomienda capacitar a los funcionarios en el ámbito legal, ya que se aplicarán leyes que rigen en la LOPDP, con el fin de garantizar un adecuado cumplimiento y así evitar posibles sanciones.

Mejorar el manejo en general de la data sensible de la DGAC, mediante la implementación de medidas que permitan minimizar el riesgo, bajo el mejor criterio, se recomienda implementar controles de seguridad adecuados, tales como cifrado de datos, autenticación sólida y medidas de prevención contra accesos no autorizados.

Implementar las medias de control acorde a la sensibilidad de los datos. Validar que los controles implementados cumplan con la LOPDP y en la medida de lo posible alinear los mismos a las buenas prácticas de COBIT mencionadas en este trabajo.

Cumplir con lo establecido en la ley, de acuerdo a las competencias de la organización, tomar en cuenta los cambios y controles sugeridos con la finalidad de evitar multas o sanciones por parte de los entes de control.

En lo que refiere al ODS 11, es importante realizar las capacitaciones adecuadas a todo el personal involucrado, sobre cómo deben ser registrados los datos en los sistemas o aplicativos informáticos de la DGAC y de cómo estos serán procesados con la finalidad de que su tratamiento sea inclusivo, seguro y sostenible.

BIBLIOGRAFIA

Antonio, P. P. (2020). *Seguridad informática (Edición 2020)*. Ediciones Paraninfo, S.A.

Cano, J. (2012). Seguridad de la información y privacidad: dos conceptos convergentes. Revista Sistemas Edición 123. Recuperado 20 de agosto de 2023, de https://acis.org.co/archivos/Revista/123/Revista%20Sistemas%20Edici%C3%B3n%20123.pdf

Carrillo, F. N. R. (2021). Los ejes centrales de la protección de datos: Consentimiento y finalidad: Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador. *USFQ Law Review*, *8*(1), Article 1. https://doi.org/10.18272/ulr.v8i1.2184

Cortés Fuentes, A. A. (2023). Propuesta de método basado en COBIT 2019, para la evaluación de procesos tecnológicos en la municipalidad de Carrillo. *InterSedes*, *24*(49), 277-306.

Investigación cualitativa | QuestionPro. (2020). Recuperado 11 de agosto de 2023, de https://www.questionpro.com/es/investigacion-cualitativa.html

Investigación Cualitativa y Cuantitativa. (2020). Significados. Recuperado 21 de agosto de 2023, de https://www.significados.com/investigacion-cualitativa-y-cuantitativa/

La Ciberseguridad IOT en la era del ransomware. (2023). *CertiSur*. Recuperado 21 de agosto de 2023, de https://www.certisur.com/noticias/la-ciberseguridad-iot-en-la-era-del-ransomware/

Moran, M. (2020). Ciudades. *Desarrollo Sostenible*. Recuperado 14 de agosto de 2023, de https://www.un.org/sustainabledevelopment/es/cities/

¿Qué es COBIT 5? Entendiendo el Gobierno de TI ó IT Governance - Genius IT Training. (2018). https://geniusitt.com/blog/que-es-cobit-5/

UASB. (2021). Protección de datos. Observatorio Ciberderechos y Tecnosociedad. Recuperado 18 de agosto de 2023, de https://www.uasb.edu.ec/ciberderechos/proteccion-de-datos/

Woody Carol (2007). Considering Operational Security Risk during System Development. Recuperado el 31 de agosto de 2023, de https://dl.acm.org/doi/10.1109/MSP.2007.3

ANEXO 1

Comparativa de los riesgos más relevantes, junto a la aplicación de la normativa vigente de LOPDP

Gestión de Riesgos		Ley Orgánica de Protección de Datos Personales	
Descripción	RIESGO	Articulo	Ley
Fallos en las copias de seguridad	Alto	Art. 12	Derecho a la información
Pérdida de confidencialidad	Bajo	Art. 13	Derecho de acceso
Manipulación malintencionada de datos/software	Medio	Art. 17	Derecho a la portabilidad
Accesos no autorizados a datos de la empresa	Medio	Art. 26	Tratamiento de datos sensibles
Corrupción de datos	Medio	Art. 33	Transferencia o comunicación de datos personales
Introducción de virus en los sistemas y troyanos	Alto	Art. 35	Acceso a datos personales por parte de terceros
Descarga de software no controlada	Bajo	Art. 38	Medidas de seguridad en el ámbito del sector público
Robo de documentos	Bajo	Art. 40	Análisis de riesgo, amenazas y vulnerabilidades
		Art. 43	Notificación de vulneración de seguridad

ANEXO 2

INFORMACIÓN DE RECOLECCIÓN DE DATOS

La siguiente encuesta está diseñada para verificar si el personal de la DGAC tiene conocimiento de cómo lleva el proceso en cuanto a un evento en la gestión del riesgo.

Preguntas	Si	No muy claro	No
¿Sabe usted cual es el proceso al encontrarse con un incidente o evento de riesgo?			
¿Sabe usted que es un evento crítico?			
¿Sabe usted quienes son los responsables en cada proceso ante algún incidente o evento de riesgo?			
¿Existe formalizado el proceso de gestión de riesgos a emplear en la Organización?			
¿Sabe usted si se ha desarrollado un plan de comunicaciones sobre el proceso de Gestión de Riesgos?			
Entre la misión del Gestor de Riesgos, o quien asuma sus responsabilidades, ¿se encuentra la de priorizar los procesos de la organización y el levantamiento del mapa de riesgos?			
¿Sabe usted cuál es el fin de las inspecciones de seguridad?			

ANEXO 3

Modelo Encuesta

Preguntas	Si	No muy claro	No
¿Sabe usted cual es el proceso al encontrarse con un incidente o evento de riesgo?	X		
¿Sabe usted que es un evento crítico?		X	
¿Sabe usted quienes son los responsables en cada proceso ante algún incidente o evento de riesgo?			X
¿Existe formalizado el proceso de gestión de riesgos a emplear en la Organización?		X	
¿Sabe usted si se ha desarrollado un plan de comunicaciones sobre el proceso de Gestión de Riesgos?			X
Entre la misión del Gestor de Riesgos, o quien asuma sus responsabilidades, ¿se encuentra la de priorizar los procesos de la organización y el levantamiento del mapa de riesgos?		X	
¿Sabe usted cuál es el fin de las inspecciones de seguridad?		X	

ANEXO 4

Enfoque de la Gestión de Riesgo junto a la LOPDP y buenas prácticas con COBIT 2019.

Gestión de Riesgos	Enfoque Riesgo	Enfoque Seguridad	LOPDP	COBIT 2019
Identificación de Datos Sensibles	La gestión de riesgos implica la identificación de los activos de información crítica y los datos personales que una organización maneja.	Esto incluye identificar qué tipos de datos personales se están recopilando, cómo se almacenan y procesan, y qué sistemas o procesos están involucrados.	Art. 26	APO12.01
Evaluación de Amenazas y Vulnerabilidades	Una vez que los datos personales se han identificado, se debe evaluar el panorama de amenazas y vulnerabilidades que podrían afectar la seguridad de estos datos.	Esto incluye analizar las posibles formas en que podrían ser comprometidos por ataques cibernéticos, errores humanos o factores externos.	Art. 40	EDM03.01
Determinación de Riesgos	Basándose en la evaluación de amenazas y vulnerabilidades, se pueden determinar los riesgos específicos para los datos personales.	Esto ayuda a priorizar las medidas de seguridad y decidir cómo mitigar o reducir esos riesgos.	Art. 40	APO12.02
Implementación de Medidas de Seguridad	La gestión de riesgos implica la implementación de medidas de seguridad adecuadas para proteger los datos personales.	Esto podría incluir la encriptación de datos, el establecimiento de controles de acceso, la implementación de sistemas de detección de intrusiones y la capacitación del personal en prácticas seguras.	Art. 38	EDM03.02
Cumplimiento Legal	La ley de protección de datos personales establece requisitos específicos para la recopilación, procesamiento y almacenamiento de datos personales.	La gestión de riesgos debe asegurarse de que las medidas de seguridad implementadas cumplan con estos requisitos legales, incluyendo la notificación adecuada a los titulares de los datos y la obtención de consentimiento cuando sea necesario.	Art. 12	APO12.01
Planificación de Respuesta a Incidentes	En caso de una brecha de seguridad o violación de datos, la gestión de riesgos debe incluir una planificación de respuesta a incidentes.	Esto implica establecer un plan claro para abordar y comunicar el incidente, minimizar el impacto y cumplir con los requisitos de notificación establecidos por la ley.	Art. 43	DSS04.02
Auditorías y Evaluaciones Continuas	La gestión de riesgos no es un proceso estático. Debe haber una supervisión constante de la efectividad de las medidas de seguridad implementadas.	Esto puede incluir auditorías regulares, pruebas de penetración y evaluaciones de riesgos para asegurarse de que la protección de los datos personales esté actualizada y adaptada a las nuevas amenazas.	Art. 40	DSS04.04

ANEXO 5

Dirección General de Aviación Civil

Dirección General de Aviación Civil (DGAC)	Fecha
Dirección de Tecnologías de la Información y Comunicación	15/7/2023

Enfoque	Estado actual	Estado futuro	Realizar bajo la LOPDP	COBIT 2019 Buenas Prácticas	Prioridad	comienzo	final	Viable	Dueño	Estado	notas
¿La DGAC cuenta con políticas de seguridad al recolectar información de sistemas informáticos o documentos físicos?	NO	Contar con Políticas	Realizar bajo el Art. 38 de la LOPDP	APO14	Crítico	18/7/2023	25/11/2023	SI	TI	En Proceso	Depende de la gobernanza de TI y de la DGAC
¿La DGAC cuentan con acuerdos de confidencialidad de la información recolectada?	NO	Contar con un acuerdo	Realizar bajo el Art. 8 de la LOPDP	APO13	Crítico	27/7/2023	30/10/2023	SI	Jurídico / TI	Análisis	
¿La DGAC cuenta con Políticas de Seguridad de Información dentro TI?	SI	Reforzar	Realizar bajo el Art.37 de la LOPDP	APO13	Importante	1/8/2023	31/12/2023	SI	TI	En Proceso	Depende de la gobernanza de TI y de la DGAC

¿Al entregar información de la DGAC se los realiza por medios autorizados?	SI	Mejorar el control	Realizar bajo el Art. 17 de la LOPDP	APO14	Importante	1/8/2023	10/8/2023	SI	TI / Planificación	Hecho	Aprobado por la dirección de TI
¿Se tiene controles de medios electrónicos a utilizar dentro de la institución para salvaguardar la información y evitar fuga de datos?	NO	Contar con Controles de Seguridad	Realizar bajo el Art. 17 de la LOPDP	APO14	Importante	1/8/2023	27/10/2023	SI	TI	Análisis	
¿El departamento de TI cuenta con controles de acceso a la información de base de datos?	SI	N/A	Realizar bajo el Art.37 de la LOPDP	APO13	Aceptable	1/8/2023	2/8/2023	SI	TI	Hecho	Sugerencia entregada al área responsable
¿Si alguna entidad sea pública o privada desea dar por terminado su gestión con la DGAC, se procede a eliminar su información de la base de datos o registros físicos si los tuviera?	NO	N/A	Realizar bajo el Art. 15 de la LOPDP	APO14	Crítico	4/8/2023	27/10/2023	SI	Jurídico / TI	Análisis	
¿La DGAC cuenta con planes de contingencia en lo que se refiere a la base de datos?	SI	Sugerir mejoras de acuerdo a la LOPDP	Realizar bajo el Art. 40 de la LOPDP	APO12	Importante	7/8/2023	8/8/2023	SI	TI / Planificación	Hecho	Sugerencia entregada al área responsable

¿La DGAC cuenta con personal responsable de seguridad de información y monitoreo de posibles vulnerabilidades dentro de la plataforma?	NO	Establecer profesionales encargados en ciberseguridad	Realizar bajo el Art. 43 de la LOPDP	MEA02	Importante	3/8/2023	23/10/2023	SI	TI / Planificación	Análisis	
¿La DGAC tiene un responsable del tratamiento de los datos personales?	NO	Establecer un responsable	Establecer responsables de acuerdo al Art. 48 de la LOPDP	APO14	Crítico	3/8/2023	30/10/2023	SI	RRHH	Análisis	Depende del área de RRHH y Planificación de la Institución