FACULTAD DE POSGRADOS

PROGRAMA DE MEJORA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) LA INSTITUCIÓN AERONAUTICA.

Autor
Gustavo Xavier Lema Pazmiño

Año
2023

FACULTAD DE POSGRADOS

PROGRAMA DE MEJORA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) LA INSTITUCIÓN AERONAUTICA.

Trabajo de Titulación presentando en conformidad con los requisitos establecidos para optar por el título de Magister en Gestión de Seguridad de la Información.

Autor
Gustavo Xavier Lema Pazmiño

Año
2023

AGRADECIMIENTO

Este trabajo de titulación agradezco a mi madre Olga Pazmiño por todo el apoyo incondicional, a mis hijas por darme las fuerzas para seguir adelante, a mis amigos agracias por las palabras de aliento. Por último, a mis compañeros de Trabajo de la DGAC por permitir formarme como profesional.

DEDICATORIA

La elaboración de este proyecto de titulación va dedicada con mucho amor y con todo mi esfuerzo, especialmente a Mi Madre Olga Pazmiño quien es la guía en mi camino, a mi familia los cuales fueron los pilares fundamentales para llegar a subir un escalón más profesionalmente.

RESUMEN

El presente trabajo de titulación consiste, en la elaboración una propuesta al programa de gestión de seguridad de la información SGSI, para la institución dedicada a la seguridad aeronáutica del país, estableciendo un programa en cual se establezca un modelo de gestión de seguridad de la información, que se alineen a los objetivos, metas, visión, misión de la institución.

Se determinará mediante el análisis la situación actual de la institución basados en un marco referencial ISO27001.2013, clasificando la información, identificando los activos críticos, y el análisis de amenazas y vulnerabilidades, identificando el nivel de madures de la institución en temas de seguridad de la información.

Conforme a los procedimientos de la evaluación se entrega a la institución los activos identificados más crítico, y se recomendara los controles que permitirán fortalecer y mejorar la gestión de la información.

ABSTRACT

The present degree work consists of preparing a proposal for the ISMS information security management program, for the institution dedicated to the country's aeronautical safety, establishing a program in which an information security management model is established., that are aligned with the objectives, goals, vision, mission of the institution.

The current situation of the institution will be determined through the analysis based on a referential framework ISO27001.2013, classifying the information, identifying critical assets, and the analysis of threats and vulnerabilities, identifying the level of maturity of the institution in security issues of information.

In accordance with the evaluation procedures, the most critical assets identified are delivered to the institution, and the controls that will strengthen and improve information management will be recommended.

INDICE

INDICE DE FIGURAS

INDICE DE TABLA

1. INTRODUCCIÓN

La información es el activo más sensible de una entidad convirtiéndose en un recurso clave para las organizaciones y por el papel que asume la tecnología desde el momento en que la información se crea hasta que se destruye, la necesidad de resguardar la información y los activos de TI de continuas amenazas a través de la mitigación de riesgos se vuelve imprescindible en las organizaciones.

Para que la seguridad de la información sea garantizada y gestionada adecuadamente, se debe hacer uso de procesos metódicos, documentados y tomado en conocimiento por toda la institución, este proceso es el que establece el SGSI (Sistema de Gestión de la Seguridad de la Información).

Día a día el número de vulnerabilidades y amenazas crece de forma exponencial, por lo que es fundamental salvaguardar los activos de información, por lo cual se gestionara un sistema eficiente que proporcione las condiciones de seguridad de la información necesarias para respaldar y ampliar los objetivos estratégicos de la institución, garantizando una gestión adecuada y operativa, alineados a la disponibilidad, confidencialidad, integridad y privacidad.

Este programa proponer un modelo de mejora a los procesos del SGSI mediante controles realizados en el sistema, fundamentando la existencia de oportunidad de mejora basadas en métrica dictadas por la metodología dictada por la ISO 27001.2013.

2. DESARROLLO DEL PROYECTO DE TITULACIÓN

2.1 Metodología

Para el desarrollo de mejora de este programa se basará en el Esquema Gubernamental de Seguridad de la Información (EGSI), estableciendo un enfoque basado en procesos, alineándose a la mejora continua que requiere de

una constante evolución para adaptarse a los cambios constantes en la institución, con el objetivo de conseguir un mayor nivel de eficacia operativa.

El EGSI está basado en la metodología ISO 27001.2013 permitiendo a la institución la evaluación del riesgo y la aplicación de controles necesarios para mitigarlos o eliminarlos, esto contribuirá al aseguramiento de la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

La ISO 27001.2013 contiene un anexo A, describe los objetivos de control y controles recomendables a la seguridad de la información, en este anexo está compuesto por 114 controles distribuidos en 14 dominios de seguridad siendo los siguientes:

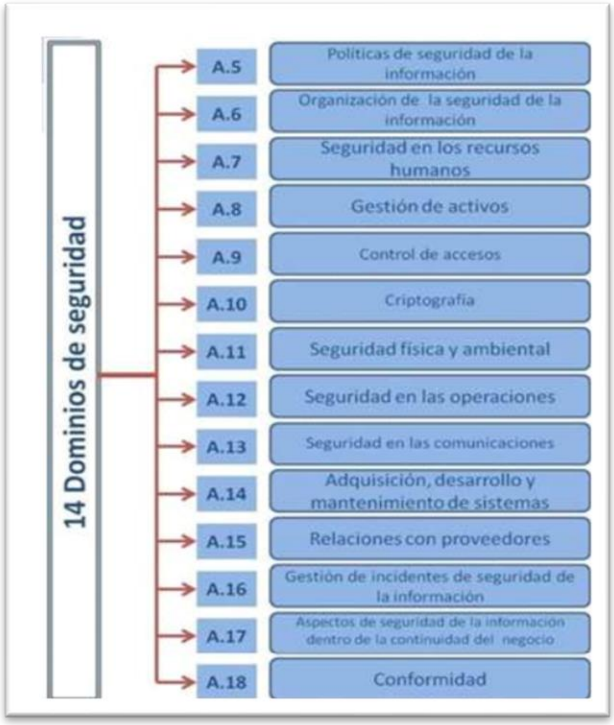


Figura 1. 14 dominios de Seguridad

Tomada de (Pozo, 2016)

Tabla 1 Dominio de Seguridad (ISO/IEC 27001.2013) Anexo A.

Dominio de Seguridad (ISO/IEC 27001.2013) Anexo A.	
A.5	Política de la seguridad de la información
A.6	Organización de la seguridad de la información
A.7	Seguridad en los recursos humanos

A.8	Gestión de activos
A.9	Control de acceso
A.10	Criptografía
A.11	Seguridad física y ambiental
A.12	Seguridad de las operaciones
A.13	Seguridad de las comunicaciones
A.14	Adquisición, desarrollo y mantenimiento de sistemas
A.15	Relaciones con proveedores
A.16	Gestión de incidentes de seguridad de la información
A.17	Aspectos de seguridad de la información de la gestión de la continuidad de negocio
A.18	Conformidad

2.2 Presupuesto

Para realizar un plan de mejora del sistema SGSI en la institución, se debe considerar un presupuesto inicial roquerito siguiente:

Tabla 2. Presupuesto

Numero	Detalle	Costo hora	(2 horas diarias)	Costo Mensual	Meses (6)	Total
1	FUNCIONARIO - OFICIAL DE SEGURIDAD	10,43	2,00	417,20	1668,80	3337,6
1	FUNCIONARIO - REPRESENTANTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	10,43	2,00	417,20	1668,80	

2.3 Alcance

2.3.1 Diagnostico.

El presente trabajo proporcionará los requisitos para establecer, implementar y mantener el mejoramiento continuo del Esquema Gubernamental de Seguridad de la Información, en la institución que pretende administrar el Sistema de Gestión de Seguridad, se basara en la Esquema Gubernamental de Seguridad de la información (EGSI) normado por la ISO/IEC 27001.2013, la cual es una

norma internacional que permitirá el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan, con el objetivo de brindar los lineamientos para que la institución inicien con la implementación del EGSI o la pueda evaluar en su situación actual.

La ISO/IEC 27001.2013, es una norma internacional emitida por la Organización Internacional de Normalización ISO. Esta norma fue publicada el 15 de octubre del año 2005 y posteriormente revisada el 25 de septiembre de 2013. Esta norma, se elaboró con el fin de conceder los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información. (Excellence, 2019).

Para el análisis respectivo se toma como referencia el estándar ISO27001.2013, con énfasis en la protección de información en diferentes formatos como son los documentos digitales, documentos físicos, terminales, y redes de acceso a la información. Esto con el fin de identificar cuan expuesta se encuentra la información crítica de una organización, la misma que es un elemento diferenciador con respecto a sus competidores ya sea a nivel local o internacional.

Evaluación

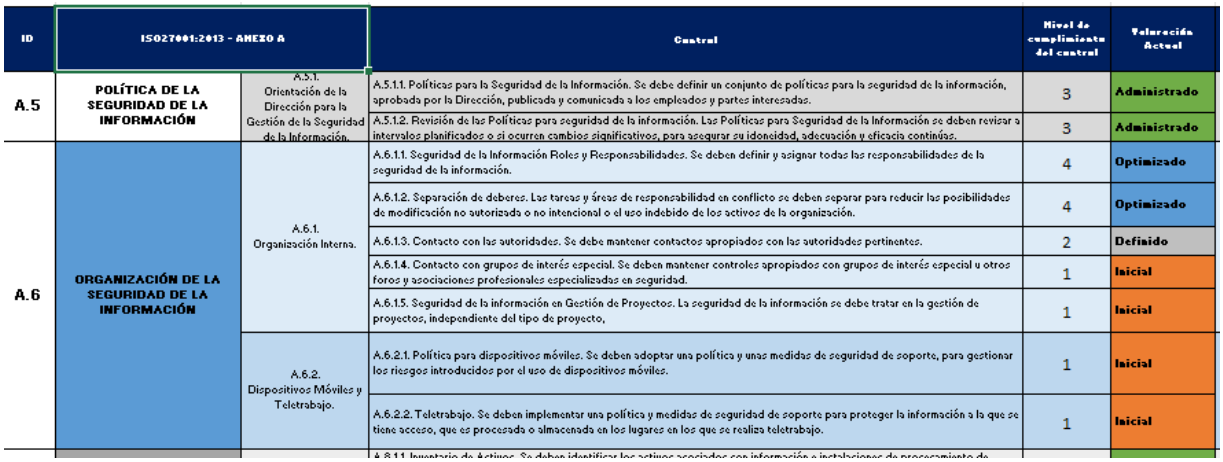
Mediante la recopilación de información y en conjunto con el Oficial de Seguridad de la institución, se ha permitido evaluar 9 dominios de 14 que dicta la norma ISO/IEC 27001.2013, los cuales se dividen en objetivos del control y su control especifico, dando una ponderación a cada objetivo de control referente a la situación actual siguiente:

Cada dominio y su control entra una retroalimentación de la situación actual del SGSI con la categorización al nivel de cumplimiento siguiente:

Tabla 3. Categorización nivel de cumplimiento

Nivel de cumplimiento		Descripción
1	Inicial	Se evidencia que existe un procedimiento sin la debida gestión, se lleva a cabo los procesos informalmente.
2	Definido	El control se encuentra aplicado y documentado, el documento se encuentra debidamente legalizado y socializado.

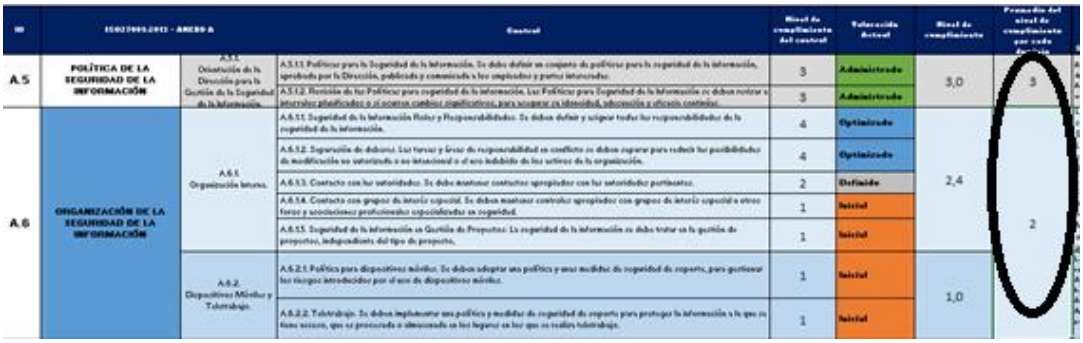
3	Administrado	El control documentado se encuentra legalizado bajo una mejora continua, medición y control del proceso.
4	Optimizado	El control cumple con las directrices gubernamentales, teniendo una innovación del proceso y su correcta optimización



ID	ISO27001:2013 - ANEXO A		Control	Nivel de cumplimiento del control	Valoración Actual
A.5	POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.	3	Administrado
			A.5.1.2. Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.	3	Administrado
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A.6.1. Organización Interna.	A.6.1.1. Seguridad de la Información Roles y Responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	4	Optimizado
			A.6.1.2. Separación de deberes. Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.	4	Optimizado
			A.6.1.3. Contacto con las autoridades. Se debe mantener contactos apropiados con las autoridades pertinentes.	2	Definido
			A.6.1.4. Contacto con grupos de interés especial. Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	1	Inicial
			A.6.1.5. Seguridad de la información en Gestión de Proyectos. La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto,	1	Inicial
		A.6.2. Dispositivos Móviles y Teletrabajo.	A.6.2.1. Política para dispositivos móviles. Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	1	Inicial
			A.6.2.2. Teletrabajo. Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	1	Inicial

Figura 2. Nivel de cumplimiento del SGSI

- Se obtiene el promedio por cada dominio evaluado, análisis del proceso Anexo, obteniendo un el promedio del nivel de cumplimiento por cada dominio.



ID	ISO27001:2013 - ANEXO A		Control	Nivel de cumplimiento del control	Valoración Actual	Nivel de cumplimiento	Promedio del nivel de cumplimiento por cada dominio
A.5	POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.	3	Administrado	3,0	3
			A.5.1.2. Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.	3	Administrado		
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A.6.1. Organización Interna.	A.6.1.1. Seguridad de la Información Roles y Responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	4	Optimizado	2,4	2
			A.6.1.2. Separación de deberes. Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.	4	Optimizado		
			A.6.1.3. Contacto con las autoridades. Se debe mantener contactos apropiados con las autoridades pertinentes.	2	Definido		
			A.6.1.4. Contacto con grupos de interés especial. Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	1	Inicial		
			A.6.1.5. Seguridad de la información en Gestión de Proyectos. La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto,	1	Inicial		
		A.6.2. Dispositivos Móviles y Teletrabajo.	A.6.2.1. Política para dispositivos móviles. Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	1	Inicial	1,0	
			A.6.2.2. Teletrabajo. Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	1	Inicial		

Figura 3. Promedio del nivel de cumplimiento por cada dominio.

- De esta manera se puede evidenciar de una manera eficiente los niveles de cumplimiento que tiene la institución frente al sistema SGSI, y que planes de acción debe tomar para mejorar su capacidad de respuesta en la seguridad de información.
  Los planes de acción se basarán conforme a los niveles de capacidad que se encuentra la institución, recomendando una mejora continua al sistema SGSI.

Tabla 4. Situación Actual Nivel de Cumplimiento

	Descripción	Situación Actual Nivel de Cumplimiento
1	POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN	Administrado
2	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Definido
3	GESTIÓN DE ACTIVOS	Administrado
4	CONTROL DE ACCESO	Administrado
5	SEGURIDAD DE LAS OPERACIONES	Definido
6	SEGURIDAD DE LAS COMUNICACIONES	Definido
7	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	Definido
8	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Definido
9	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	Definido

Esa tabla está definida según la Tabla 3. Categorización nivel de cumplimiento.

Tabla 5. Numero de Controles Evaluados ISO27001:2013

Nro. de Controles Evaluados ISO27001:2013	Estado de Control Evaluado
28	Inicial
29	Definido
19	Administrado
0	Optimizado

Figura 4. Estado Nro. de Controles Evaluados (ISO27001:2013)

- El resumen de la metodología implementada se evidencia el estado actual general y las oportunidades de mejora, las cuales se encuentran en Anexo.

2.3.2 Apetito al riesgo de la institución

El apetito al riesgo es la cantidad de riesgo que una organización está dispuesta a asumir para alcanzar sus objetivos estratégicos. Conoce aquí por qué es importante.

En la gestión de riesgos, el apetito es lo primero que debe establecerse, ya que al determinar el nivel de riesgo que enfrentará la empresa, se conocerá qué tantos recursos y esfuerzos se requieren para manejarlo y mitigar un posible impacto. De esa forma se previenen los riesgos financieros. Un ejemplo de esto son las inversiones. (Salazar, 2021).

Para poder clasificar la información de la institución y poder evaluar los activos de información más críticos, es imprescindible identificar los riesgos que enfrentara la institución ante un incidente de seguridad informática afectando a la integridad de la información en los pilares fundamentales de la confidencialidad, integridad, disponibilidad y privacidad.

Para lo cual se detalla los objetivos institucionales frente a los servicios aeronáuticos que brinda a nivel nacional y su respectivo modulador:

Tabla 6. Modulador de impacto

Impacto	Aversión	Neutral	Agresivo
Pérdidas Financieras para el Estado Ecuatoriano	X		
Interacción de las operaciones aeronáuticas parciales y/o totales	X		
Demandas Judiciales / afectación Legal (Nacional y/o Internacional)		X	X
Perdida / Degradación de la Imagen Institucional	X	X	
Sumarios administrativos (Despido de personal)			X

Una vez definido el modelador apetito al riesgo de cada objetivo institucionales frente a los servicios aeronáuticos que este brinda, se procede a evaluar los niveles de riesgo que la institución está dispuesta a alcanzar.

- Riesgo: Perdidas Financieras para el Estado Ecuatoriano.

✓ Insignificante: No aplica para la institución
✓ Menor: Perdidas menores del 5% de los valores netos por el servicio de trasporte aéreo.
✓ Moderado: Perdidas mayores al 5 % y menores al 10 % de los valores netos por el servicio de trasporte aéreo.
✓ Mayor: Perdidas mayores al 10 % y menores al 15 % de los valores netos por el servicio de trasporte aéreo.
✓ Catastrófico: Perdidas mayores al 20 % de los valores netos por el servicio de trasporte aéreo.

- Riesgo: Interrupción de las operaciones parciales y/o totales.

✓ Insignificante: No aplica para la institución.
✓ Menor: No aplica para la institución.
✓ Moderado: Perdida del servicio de 0 a 5 minutos.
✓ Mayor: Perdida del servicio de 5 a 15 minutos.
✓ Catastrófico: Perdida del servicio de Mayor a 15 minutos.

- Riesgo: Demandas Judiciales / afectación Legal (Nacional y/o Internacional).

✓ Insignificante: No aplica para la institución
✓ Menor: Reclamos por parte del usuario por la no disponibilidad de los servicios.
✓ Moderado: Sanciones legales por la no disponibilidad de los servicios (Nivel Nacional).
✓ Mayor: Sanciones legales por la no disponibilidad de los servicios (Nivel Internacional).
✓ Catastrófico: Sanciones legales por la no disponibilidad de los servicios (Estado Ecuatoriano)

- Riesgo: Perdida / Degradación de la Imagen Institucional

✓ Insignificante: No aplica para la institución
✓ Menor: No aplica para la institución
✓ Moderado: Pérdida de confianza por partes de los usuarios que utilizan los servicios.
✓ Mayor: Pérdida de confianza de por parte de las aerolíneas aéreas que utiliza los servicios.
✓ Catastrófico: Pérdida de confianza por partes del Estado Ecuatoriano.

Sumarios administrativos (Despido de funcionarios técnicos).

✓ Insignificante: No aplica para la institución
✓ Menor: No aplica para la institución
✓ Moderado: (1) un funcionario técnico al año.

- ✓ Mayor: (2) dos funcionarios técnicos al año.
- ✓ Catastrófico: (3) tres funcionarios técnicos al año.

2.3.3 Clasificación de la información e inventario de activos.

Una vez identificados los riesgos que la organización puede asumir, es posible clasificar la información para lo cual se identificaron las entidades siguientes:

- Pilotos Aéreos:

  Información General del Piloto: Nombres de la Persona Apellido Paterno, Apellido Materno, Correo Electrónico, Fecha Nacimiento (al posicionar el cursor en el campo, se despliega un selector de fecha), Estado Civil País de Nacionalidad, Lugar de Nacimiento (Cuidad-país).

  Información de licencia del piloto: Tipo de licencia, grupo de licencia, habilitación de categoría, habilitación de clase de avión (avión/helicóptero), habilitación de tipo de avión, Cumplimiento de Chequeo Requerido, Competencia Militar Obtenida, Graduado de Curso Aprobado, Poseedor de Licencia Extranjera Emitida Por, Cumplimiento de Programa de Entrenamiento Aprobado de Transportador Aéreo.
  Información de documentación habilitante: bitácora de vuelo, cedula de ciudadanía, certificado de curso de entrenamiento, certificado médico, certificado de escuela de aviación, certificado de horas de vuelo nocturnas.

- Compañías Aéreas:

  Información general de Compañías aéreas (nacional o extranjera): Sigla IATA, Código OACI, nombre, país de origen cuidad de origen, comercial, teléfono, dirección, vigencia COA, email.

  Información del representante técnico de Compañías aéreas: Nombre del representante técnico, cargo del representante técnico, cuidad de residencia, dirección, teléfono, email.

  Información Legal de las compañías aéreas: Representante legal, cargo del representante legal, cuidad de residencia, dirección, teléfono email.

  Información general de las aeronaves de las Compañías Aéreas: siglas de la compañía, teléfono, nombre de la compañía, siglas técnicas, marca, modelo/tipo, matricula número de serie, numero de certificación

aeronáutica, estado, región, base de operación, destino de uso, aprobado para pasajeros o carga).

Información técnica de las aeronaves de las Compañías Aéreas: año de fabricación, unidades de peso, peso máximo de aterrizaje, peso vacío, condiciones de vuelo, peso máximo de la estructura, numero Max. Pasajeros, categoría, numero Max. De tripulantes, autonomía, número de personas extras, capacidad de galones de combustibles, galones/hora, equipos electrónicos, equipos de emergencia.

Información de validación de certificaciones de las aeronaves de las Compañías Aéreas: fecha de otorgación del certificado, fecha de vencimiento del certificado, fecha de vencimiento del seguro, fecha del último peso/balance, fecha del próximo balance, fecha de la última inspección, lugar de la inspección, fecha de ingreso al país, último país, ultimo propietario.

Información de planes de vuelo de las aeronaves de las Compañías Aéreas: prioridad del vuelo, destinos, hora del depósito, remitente, identificación de la aeronave, reglas del vuelo, tipo de vuelo, tipo de aeronave, categoría de turbulencia, equipo, aeródromo de salida, hora, velocidad del crucero, nivel, ruta, aeródromo de destino.

Información meteorológica de la Compañías Aéreas: Id, usuarios, Presión Atmosférica, Temperatura y Humedad, Viento, vis, Precipitación.

- Funcionarios:

Información general del funcionario: Información General del funcionario: Identificación, apellidos, nombres, estado (contrato, nombramiento provisional, nombramiento permanente), Estado Civil, Sexo, fecha de ingreso a la institución, libreta militar, nacionalidad, numero del IESS, fecha de nacimiento, fecha de matrimonio, provincia de nacimiento, parroquia de nacimiento, domicilio, tipo académico, teléfono (convencional, celular, emergencia), mail institucional y personal.

Información de datos físicos del funcionario: Información física del funcionario: talla de zapatos, talla de saco, talla de pantalón, talla de falda, talla de botas, talla de overall, talla de guantes, talla de casco, talla de mandil, color de piel, color de ojos, color de cabello, casa propia, terreno propio, vive con.

Información Médica del funcionario: tipo de sangre, alergias, enfermedades pasadas, cirugías realizadas, condición física, observaciones médicas.

Información familiar del funcionario: cedula de identidad, parentesco, nombre, apellidos, fecha de nacimiento, observaciones.

Información financiera del funcionario: Información financiera del funcionario: Ingresos mensuales, gastos funcionario mensuales, pasivos, activos, cargas familiares.

- Proveedores:

Información de contacto del proveedor: Información que permita contactar a los proveedores, ya sea de manera física o por medios tecnológicos, Ejemplo: país, ciudad, dirección física de la empresa, número de teléfono convencional/ celular, email, pagina.

Información Legal del Proveedor: Información que permita identificar al proveedor, si es persona natural o jurídica. Ejemplo: Registro de la constitución de la empresa, RUC, representante legal, accionistas.

Información Financiera del proveedor: Información referente a préstamos, deudas por pagar, deudas por cobrar; así como cuentas bancarias o formas de pago.

Identificado el tipo de información que la institución, se procede a evaluar cada entidad con respecto a los 4 pilares fundamentales: confidencialidad, integridad, disponibilidad y privacidad.

Tabla 7. Identificación del riesgo para el tipo de información.

Entidad	Nombre del tipo de información	Evaluación de Confidencialidad	Evaluación de Integridad	Evaluación de Disponibilidad	Evaluación de Privacidad
Pilotos Aéreos	Información General del Piloto	Menor	Moderado	Menor	Menor
	Información de licencia del piloto	Menor	Mayor	Menor	Menor
	Información de documentación habilitante	Catastrófico	Catastrófico	Catastrófico	Mayor
Compañías Aéreas	Información general de Compañías aéreas (nacional o extranjera)	Menor	Menor	Menor	Menor
	Información del representante técnico de Compañías aéreas	Menor	Menor	Insignificante	Menor
	Información Legal de las compañías aéreas	Moderado	Menor	Insignificante	Menor

	Información general de las aeronaves de las Compañías Aéreas	Menor	Menor	Mayor	Moderado
	Información técnica de las aeronaves de las Compañías Aéreas	Insignificante	Menor	Mayor	Moderado
	Información de validación de certificaciones de las aeronaves de las Compañías Aéreas	Moderado	Mayor	Catastrófico	Moderado
	Información de planes de vuelo de las aeronaves de las Compañías Aéreas	Catastrófico	Catastrófico	Catastrófico	Catastrófico
	Información meteorológica de la Compañías Aéreas	Mayor	Catastrófico	Catastrófico	Mayor
Funcionarios	Información general del funcionario	Insignificante	Moderado	Menor	Insignificante
	Información de datos físicos del funcionario	Menor	Menor	Menor	Menor
	Información Médica del funcionario	Menor	Moderado	Menor	Menor
	Información familiar del funcionario	Menor	Menor	Menor	Insignificante
	Información financiera del funcionario	Catastrófico	Catastrófico	Mayor	Menor
Proveedores	Información de contacto del proveedor	Menor	Menor	Insignificante	Insignificante
	Información Legal del Proveedor	Menor	Moderado	Insignificante	Menor
	Información Financiera del proveedor	Menor	Menor	Insignificante	Menor

Se puede establecer las entidades de mayor impacto para la institución, la cual se encuentra evaluada bajo un nivel de aceptación evidenciando el activo de mayor riesgo.

Entidad	Nombre del tipo de informacion	Nivel de criticidad	Activo de Informaciòn	Componente	Evaluación	Calificaciòn
Pilotos Aéreos	Información General del Piloto	Aceptable	sistema_(SIPA) Sistema de Información del Personal Aeronautico	Base de Datos	3	Critico
	Información de licencia del piloto	Aceptable		web service	2	Medio
	Información de documentación habilitante del piloto	Aceptable		Sistema Operativo	1	Bajo
Compañias Aéreas	Información general de Compañías aéreas (nacional o extranjera)	Aceptable	Servidor_Sistema_Integrado (CORE)	DB2	3	Critico
	Información del representante técnico de Compañías aéreas	Aceptable		DB2	2	Medio
	Información Legal de las compañías aéreas	Aceptable		DB2	3	Critico
	Información general de las aeronaves de las Compañías Aéreas	Aceptable		DB2	1	Bajo
	Información técnica de las aeronaves de las Compañías Aéreas	Aceptable		DB2	2	Medio
	Información de validación de certificaciones de las aeronaves de las Compañías Aéreas	Aceptable		DB2	2	Medio
	Información de planes de vuelo de las aeronaves de las Compañías Aéreas	Catastrofico	sistema_(IFIS) Internet información flight service	Base de Datos	3	Critico
	Información meteorológica de la Compañías Aéreas	Catastrofico		web service	3	Critico
Funcionarios	Información general del funcionario	Aceptable	Carpeta_compartida	Sistema Operativo	2	Medio
	Información de datos físicos del funcionario	Aceptable		Servidor físico	2	Medio
	Información Médica del funcionario	Aceptable		File Server	1	Bajo
	Información familiar del funcionario	Aceptable			2	Medio
	Información financiera del funcionario	Aceptable			1	Bajo
Proveedores	Información de contacto del proveedor	Aceptable	Carpeta_compartida	Sistema Operativo	1	Bajo
	Información Legal del Proveedor	Aceptable			1	Bajo
	Información Financiera del proveedor	Aceptable			2	Medio

Figura 5. Activos de información y evaluación.

Según el análisis realizado el activo información mas critico es el **sistema_(IFIS) Internet información flight service** con su “Base de Datos”, para lo cual, este será el activo a ser evaluado (amenazas y vulnerabilidades), para posteriormente corregirla mediante implementación de controles.

2.3.4 Evaluación del activo en base al riesgo.

Una vez identificado el activo más crítico (sistema_(IFIS) Internet información flight service), cuya valoración logro el nivel más alto con puntaje (**catastrófico**).

Dicho activo (sistema_(IFIS) Internet información flight service), tiene como funcionalidad principal la administración los planes de vuelo de las aeronaves de las Compañías Aéreas ya sean nacionales e internacionales, los mismos que se componen de la manera siguiente:

- Servidor físico: Es un servidor basado en hardware encargado de almacenar la información que es generada por el sistema_(IFIS) Internet información flight service.
- base de datos: Es un activo de almacenamiento para una gran cantidad de datos, relacionados y estructurados, la cual se puede acceder y cumplir las funcionalidades de administrar desde el sistema_(IFIS) Internet información flight service.
- web service: Es la intercomunicación e interoperabilidad el cual interactúa con otros sistemas o activos de información.
- Sistema Operativo: Es un programa que, después de ser cargado inicialmente en el servidor por un programa de arranque, administra el sistema_(IFIS) Internet información flight service instalado.

Se clasifica los componentes para los activos más críticos, con la finalidad de evaluar el riesgo e impacto hacia la institución resultando lo siguiente:

Tabla 8. Categorización a los componentes del activo de información sistema_(IFIS) Internet información flight service instalado.

Entidad	Nombre del tipo de información	Activo de Información	Componente	Calificación
Compañías Aéreas	Información de planes de vuelo de las aeronaves de las Compañías Aéreas	sistema_(IFIS) Internet información flight service	base de datos	Crítico
			web service	Alto

Podemos evidenciar que el activo más critico es la Base de Datos, se analizará la respectiva amenazas y vulnerabilidades que las conlleva, apoyado en metodologías dictadas por Margerit V3, definida como “un método formal para investigar los riesgos que soportan los Sistemas de Información y para

recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos." (Mejía, 2021)

sistema_(IFIS) Internet información flight service “Base de Datos”

[E] Errores y fallos no intencionados:

[E.1] Errores de los usuarios:

- Interfaz de usuario sofisticada.
- Falta de documentación.
- La configuración de parámetros no es correcta.
- La fecha no es correcta.
- Capacitación de software insuficiente.
- Uso inadecuado del software Falta de conciencia de seguridad.

[E.2] Errores del administrador:

- Interfaz de usuario sofisticada.
- Falta de documentación.
- La configuración de parámetros no es correcta.
- Capacitación de software insuficiente.
- Uso indebido del software.
- Interfaz de usuario sofisticada.
- Falta de conciencia de seguridad.

[E.3] Errores de monitorización (log):

- Sin registro de auditoría.
- Programa faltante Faltan entradas en los registros del administrador y del operador.
- Seguimiento de los recursos de procesamiento de la información.

[E.4] Errores de configuración:

- Falta de documentación.
- La configuración de parámetros no es correcta.
- Insuficiente formación en seguridad.
- Uso indebido del software.
- Falta de conciencia de seguridad.

[E.8] Difusión de software dañino:

- Líneas de comunicación desprotegidas.
- Tráfico sensible sin protección.
- Arquitectura de red insegura.
- Transferencia clara de contraseñas.
- falta de mecanismos de seguimiento.

[E.14] Escapes de información:

- Habilitar de niveles de servicios innecesarios.
- Falta de mecanismos de seguimiento.
- Líneas de comunicación desprotegidas Tráfico sensible desprotegido.
- Empleados desmotivados.

[E.15] Alteración accidental de la información:

- La interfaz de usuario compleja carece de documentación.
- La configuración de parámetros es incorrecta.
- Capacitación de software insuficiente.
- Uso indebido del software.
- Falta de conciencia de seguridad.

[E.18] Destrucción de información:

- Interfaz de usuario compleja
- Falta de documentos.
- Configuración de parámetros incorrectos.
- Capacitación de software insuficiente.
- Uso inadecuado del software
- Falta de conciencia de seguridad.

[E.19] Fugas de información:

- Interfaz de usuario compleja
- Falta de documentos.
- Configuración de parámetros incorrectos.
- Capacitación de software insuficiente.
- Uso inadecuado del software • Falta de conciencia de seguridad.

[E.20] Vulnerabilidades de los programas (software):

- Interfaz de usuario sofisticada.
- Sin copias de seguridad.
- Falta de documentos.
- Configuración de parámetros incorrectos.
- Capacitación de software insuficiente.
- Uso indebido del software.
- Falta de conciencia de seguridad.

[E.21] Errores de mantenimiento / actualización de programas (software):

- Falta de documentación.
- Capacitación de software insuficiente.
- Falta de procedimientos de control de cambios
- Acuerdos de nivel de servicio inexistentes o inadecuados.
- La especificación del desarrollador es incompleta o poco clara. Falta de redundancia, copia única.

[E.24] Caída del sistema por agotamiento de recursos:

- Falta de un programa de reemplazo regular.
- Falta de mecanismo de monitoreo Falta de plan de continuidad.
- Mantenimiento de medios insuficiente/instalación fallida.

[A] Ataques intencionados

[A.3] Manipulación de los registros de actividad (log):

- Falta de procedimientos para reportar vulnerabilidades de seguridad.
- Falta de pruebas periódicas de gestión de conexiones de redes públicas vulnerables.
- Error al generar mensajes de control.
- Falta de procedimientos formales para el control de la documentación del SGSI. • Falta de procedimientos formales para monitorear el registro del SGSI.
- Sobre el mal tiempo de uso de datos en la aplicación.
- Software ampliamente distribuido.
- Ausencia o débil implementación de auditoría interna.
- Sin registro de auditoría.
- Falta de procedimientos formales de registro y exclusión de usuarios.
- Falta de procedimientos de identificación y evaluación de riesgos.

- Falta de un proceso formal de revisión (supervisión) de los derechos de acceso.

[A.4] Manipulación de la configuración:

- Falta de procedimientos para reportar vulnerabilidades de seguridad.
- Falta de gestión regular.
- Conexiones de red pública no seguras.
- Error al generar mensajes de control.
- Falta de procedimientos formales para verificar la documentación del SGSI.
- Falta de procedimientos formales para monitorear el registro del SGSI.
- Sobre el mal tiempo de uso de datos en la aplicación.
- Software ampliamente distribuido.
- Falta o débil implementación de la auditoría interna.
- No hay registro de auditoría.
- Falta de procedimientos formales de registro y exclusión de usuarios.
- Falta de procedimientos de identificación y evaluación de riesgos.
- Falta de un proceso formal de revisión (supervisión) de los derechos de acceso.

[A.5] Suplantación de la identidad del usuario:

- Falta de mecanismos de identificación y autenticación, como la autenticación de usuarios.
- Tablas de contraseñas desprotegidas.
- Mala gestión de contraseñas.

[A.6] Abuso de privilegios de acceso:

- Asignación incorrecta de derechos de acceso.
- No "cerrar sesión" al salir de la estación de trabajo.
- Falta de auditorías periódicas (seguimiento).
- Sin registro de auditoría.
- Falta de procedimientos de seguimiento de los recursos de procesamiento de información.
- Falta de procedimientos formales de registro y exclusión de usuarios.
- Falta de procedimientos para la identificación y evaluación de riesgos.
- Falta de un proceso formal de revisión (supervisión) de acceso.
- No hay mensajes de error en los registros de administrador y operador.
- Pruebas de software faltantes o insuficientes.

- Errores de software conocidos.
- Falta de mecanismos de identificación y autenticación, como la autenticación de usuarios.
- Mala gestión de contraseñas.
- Tablas de contraseñas vulnerables.

[A.8] Difusión de software dañino:

- Líneas de comunicación desprotegidas.
- Tráfico sensible sin protección.
- Arquitectura de red insegura.
- Falta de herramientas de ciberseguridad.

[A.10] Alteración de secuencia:

- Líneas de comunicación desprotegidas.
- Tráfico sensible desprotegido Arquitectura de red insegura.
- Falta de herramientas de ciberseguridad.
- Líneas de comunicación desprotegidas.
- No hay tráfico sensible.
- Arquitectura indefinida de red.
- Enviar contraseñas en texto claro.

[A.11] Acceso no autorizado:

- Otorgamiento incorrecto de derechos de acceso: no hay "terminación de sesión" al abandonar la estación de trabajo.
- Falta de auditorías periódicas (seguimiento).
- Sin registro de auditoría.
- Falta de procedimientos de seguimiento de los recursos de procesamiento de información.
- Falta de procedimientos formales de registro y exclusión de usuarios.
- Falta de procedimientos de identificación y evaluación de riesgos.
- Falta de un proceso formal de revisión (supervisión) de acceso.
- No hay mensajes de error en los registros de administrador y operador.
- Pruebas de software faltantes o insuficientes. • Errores de software conocidos. • Falta de mecanismos de identificación y autenticación, como la autenticación de usuarios.
- Mala gestión de contraseñas.
- Tablas de contraseñas vulnerables.

[A.15] Modificación deliberada de la información:

- Falta de procedimientos para reportar brechas de seguridad
- Falta de revisión periódica de procedimiento por parte de la gerencia.
- Conexiones de red pública no seguras.
- Error al generar mensajes de control.
- Falta de procedimientos formales para verificar la documentación del SGSI - Falta de procedimientos formales para monitorear el registro del SGSI.
- Sobre la vida útil de los datos erróneos en la aplicación.
- Software generalizado: falta de auditoría interna o está mal implementada.
- Sin registro de auditoría.
- Falta de procedimientos formales de registro y exclusión de usuarios.
- Falta de procedimientos de identificación y evaluación de riesgos.
- Falta de un proceso formal de revisión (supervisión) de acceso.

[A.18] Destrucción de información:

- Líneas de comunicación desprotegidas.
- Tráfico sensible sin protección.
- Arquitectura de red insegura.
- Falta de herramientas de ciberseguridad.
- Líneas de comunicación desprotegidas.
- Tráfico sensible desprotegido Arquitectura de red insegura.
- Enviar contraseñas en texto claro.

[A.19] Divulgación de información:

- Falta de procedimientos para reportar vulnerabilidades de seguridad.
- Falta de gestión regular.
- Conexiones de red pública no seguras.
- Error al generar mensajes de control.
- Falta de procedimientos formales para verificar la documentación del SGSI. Falta de procedimientos formales para monitorear el registro del SGSI.
- Sobre el mal tiempo de uso de datos en la aplicación.
- Amplia distribución de software de auditoría interna.
- Falta de implementación o implementación deficiente.
- Sin registro de auditoría.
- Falta de procedimientos formales de registro y exclusión de usuarios.
- Falta de procedimientos de identificación y evaluación de riesgos.
- Falta de un proceso formal de revisión (supervisión) de acceso.

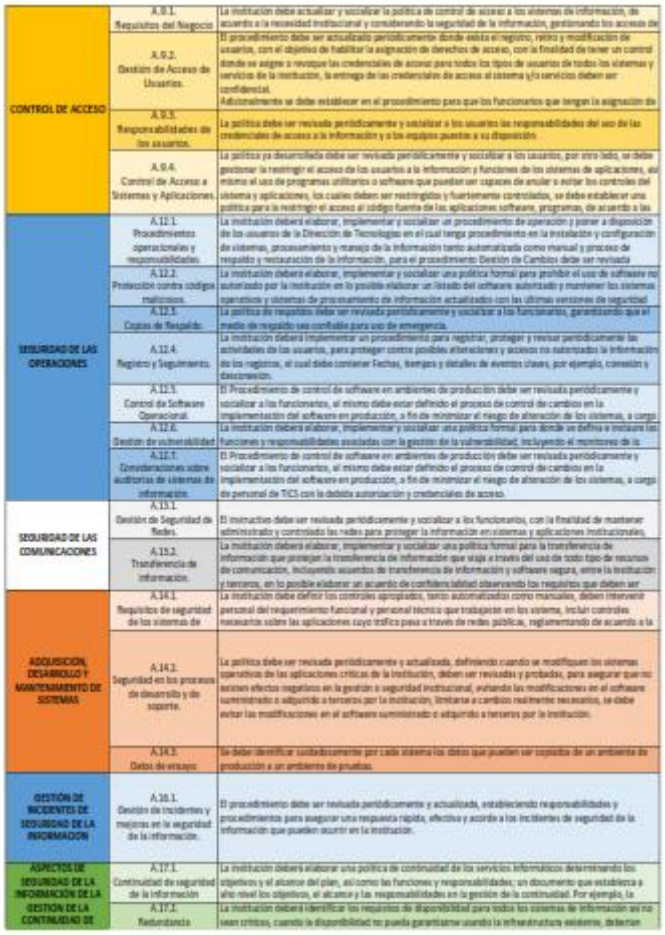
[A.24] Denegación de servicio:

- Falta de procedimientos para reportar vulnerabilidades de seguridad.
- Falta de gestión regular.
- Conexiones de red pública no seguras.
- Error al generar mensajes de control.
- Falta de procedimientos formales para verificar la documentación del SGSI. Falta de procedimientos formales para monitorear el registro del SGSI.
- Sobre el mal tiempo de uso de datos en la aplicación.
- Amplia distribución de software de auditoría interna.
- Falta de implementación o implementación deficiente.
- Sin registro de auditoría.
- Falta de procedimientos formales de registro y exclusión de usuarios.
- Falta de procedimientos de identificación y evaluación de riesgos.
- Falta de un proceso formal de revisión (supervisión) de acceso.

2.3.5 Políticas de Alto Nivel

La institución al ser de la función ejecutiva, esta regida por el ente regulador MINTEL el cual debe acatar sus acuerdos ministeriales emitidos para fortalecer

y programas del SGSI, para los cual se establece políticas de alto nivel.



CONTROL DE ACCESO	A.9.1. Requisitos del Negocio	La institución debe actualizar y socializar la política de control de acceso a los sistemas de información, de acuerdo a la necesidad institucional y considerando la seguridad de la información, gestionando los accesos de
	A.9.2. Gestión de Acceso de Usuarios.	El procedimiento debe ser actualizado periódicamente donde exista el registro, retiro y modificación de usuarios, con el objetivo de habilitar la asignación de derechos de acceso, con la finalidad de tener un control donde se asigne o revoque las credenciales de acceso para todos los tipos de usuarios de todos los sistemas y servicios de la institución, la entrega de las credenciales de acceso al sistema y/o servicios deben ser confidencial. Adicionalmente se debe establecer en el procedimiento para que los funcionarios que tengan la asignación de
	A.9.3. Responsabilidades de los usuarios.	La política debe ser revisada periódicamente y socializar a los usuarios las responsabilidades del uso de las credenciales de acceso a la información y a los equipos puestos a su disposición
	A.9.4. Control de Acceso a Sistemas y Aplicaciones.	La política ya desarrollada debe ser revisada periódicamente y socializar a los usuarios, por otro lado, se debe gestionar la restringir el acceso de los usuarios a la información y funciones de los sistemas de aplicaciones, así mismo el uso de programas utilitarios o software que puedan ser capaces de anular o evitar los controles del sistema y aplicaciones, los cuales deben ser restringidos y fuertemente controlados, se debe establecer una política para la restringir el acceso al código fuente de las aplicaciones software, programas, de acuerdo a las
SEGURIDAD DE LAS OPERACIONES	A.12.1. Procedimientos operacionales y responsabilidades.	La institución deberá elaborar, implementar y socializar un procedimiento de operación y poner a disposición de los usuarios de la Dirección de Tecnologías en el cual tenga procedimiento en la instalación y configuración de sistemas, procesamiento y manejo de la información tanto automatizada como manual y proceso de respaldo y restauración de la información, para el procedimiento Gestión de Cambios debe ser revisada
	A.12.2. Protección contra código malicioso.	La institución deberá elaborar, implementar y socializar una política formal para prohibir el uso de software no autorizado por la institución en lo posible elaborar un listado del software autorizado y mantener los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad
	A.12.3. Copias de Respaldo.	La política de respaldo debe ser revisada periódicamente y socializar a los funcionarios, garantizando que el medio de respaldo sea confiable para uso de emergencia.
	A.12.4. Registro y Seguimiento.	La institución deberá implementar un procedimiento para registrar, proteger y revisar periódicamente las actividades de los usuarios, para proteger contra posibles alteraciones y accesos no autorizados la información de los registros, el cual debe contener Fechas, tiempos y detalles de eventos claves, por ejemplo, conexión y desconexión.
	A.12.5. Control de Software Operacional.	El Procedimiento de control de software en ambientes de producción debe ser revisada periódicamente y socializar a los funcionarios, el mismo debe estar definido el proceso de control de cambios en la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas, a cargo
	A.12.6. Gestión de vulnerabilidad	La institución deberá elaborar, implementar y socializar una política formal para donde se defina e incluyan las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad, incluyendo el monitoreo de la
	A.12.7. Consideraciones sobre auditorías de sistemas de información	El Procedimiento de control de software en ambientes de producción debe ser revisada periódicamente y socializar a los funcionarios, el mismo debe estar definido el proceso de control de cambios en la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas, a cargo de personal de TICS con la debida autorización y credenciales de acceso.
SEGURIDAD DE LAS COMUNICACIONES	A.13.1. Gestión de Seguridad de Redes.	El instructivo debe ser revisada periódicamente y socializar a los funcionarios, con la finalidad de mantener administrado y controlado las redes para proteger la información en sistemas y aplicaciones institucionales,
	A.13.2. Transferencia de información.	La institución deberá elaborar, implementar y socializar una política formal para la transferencia de información que proteja la transferencia de información que viaja a través del uso de todo tipo de recurso de comunicación, incluyendo acuerdos de transferencia de información y software segura, entre la institución y terceros, en lo posible elaborar un acuerdo de confidencialidad observando los requisitos que deben ser
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	A.14.1. Requisitos de seguridad de los sistemas de	La institución debe definir los controles apropiados, tanto automatizados como manuales, deben intervenir personal del requerimiento funcional y personal técnico que trabajaran en los sistema, incluir controles necesarios sobre las aplicaciones cuyo tráfico pasa a través de redes públicas, reglamentando de acuerdo a la
	A.14.2. Seguridad en los procesos de desarrollo y de soporte.	La política debe ser revisada periódicamente y actualizada, definiendo cuando se modifiquen los sistemas operativos de las aplicaciones críticas de la institución, deben ser revisadas y probadas, para asegurar que no existen efectos negativos en la gestión o seguridad institucional, evitando las modificaciones en el software suministrado o adquirido a terceros por la institución, limitarse a cambios realmente necesarios, se debe evitar las modificaciones en el software suministrado o adquirido a terceros por la institución.
	A.14.3. Datos de ensayo	Se debe identificar cuidadosamente por cada sistema los datos que pueden ser copiados de un ambiente de producción a un ambiente de pruebas.
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información.	El procedimiento debe ser revisada periódicamente y actualizada, estableciendo responsabilidades y procedimientos para asegurar una respuesta rápida, efectiva y acorde a los incidentes de seguridad de la información que pueden ocurrir en la institución.
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE	A.17.1. Continuidad de seguridad de la información	La institución deberá elaborar una política de continuidad de los servicios informáticos determinando los objetivos y el alcance del plan, así como las funciones y responsabilidades; un documento que establezca a alto nivel los objetivos, el alcance y las responsabilidades en la gestión de la continuidad. Por ejemplo, la
	A.17.1. Redundancia	La institución deberá identificar los requisitos de disponibilidad para todos los sistemas de información así no sean críticos, cuando la disponibilidad no pueda garantizarse usando la infraestructura existente, deberían

Figura 6. Políticas de Alto Nivel

Para encargarse de los procesos y políticas, se determina roles dentro de la institución las cuales son dictadas por el Ministerio de Telecomunicaciones y de la Sociedad de la Información, a través del Acuerdo Ministerial No.025-2019 expidió el Esquema Gubernamental de Seguridad de la Información - EGSI (versión 2.0), el cual es de implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva (APC).

En el Artículo 5 de dicho Acuerdo Ministerial menciona que: *“La máxima autoridad designará al interior de la Institución, un Comité de Seguridad de la Información (CSI), que estará integrado por los responsables de las siguientes áreas o quienes hagan sus veces: Talento Humano, Administrativa, Planificación y Gestión Estratégica, Comunicación Social, Tecnologías de la Información, Unidades Agregadores de Valor y el Área Jurídica participará como asesor”*

En el Artículo 7 de dicho Acuerdo Ministerial menciona que: *"El Comité de Seguridad de la Información (CSI) designará al interior de su Institución a un funcionario como Oficial de Seguridad de la Información (OSI).".*

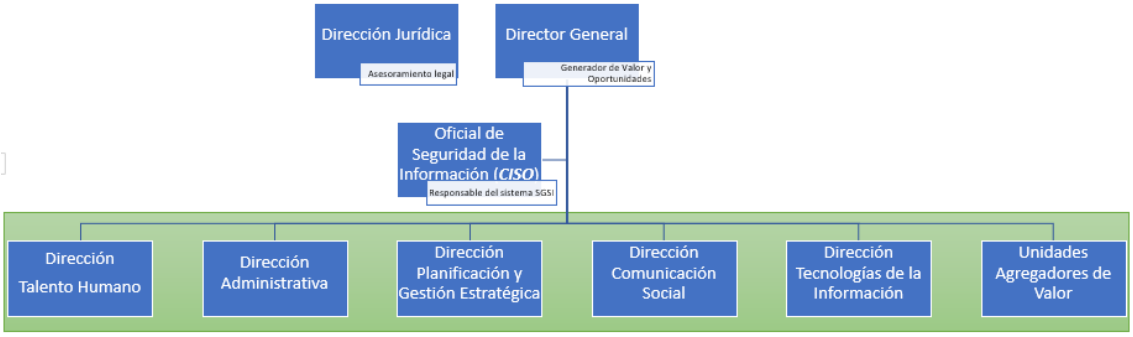


Figura 7. Roles y responsabilidades de la institución para el SGSI.

Artículo 6. del Acuerdo Ministerial No.025-2019, indica las responsabilidades del Comité de Seguridad de la Información (MINTEL, 2010)

- Gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución.

- Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto.

- Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI. e) Promover la difusión de la seguridad de la información dentro de la institución.

- Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.

- El comité deberá convocarse bimensualmente o cuando las circunstancias lo ameriten, se deberá llevar registros y actas de las reuniones.

- Informar a la máxima autoridad los avances de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).
- Reportar a la máxima autoridad las alertas que impidan la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

- Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

Artículo 8. del Acuerdo Ministerial No.025-2019, indica las responsabilidades del Oficial de Seguridad de la Información (MINTEL, 2010)

- Identificar todas las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI.

- Generar propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información (EGSI).

- Asesorar a los funcionarios en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas.

- Elaborar el Plan de concienciación en Seguridad de la Información basado en el Esquema

- Gubernamental de Seguridad de la Información (EGSI).

- Elaborar un plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas.

- Coordinar la elaboración del Plan de Continuidad de Seguridad de la Información.

- Orientar y generar un procedimiento adecuado para el manejo de los incidentes de seguridad de la información presentados al interior de la institución.

- Coordinar la gestión de incidentes de seguridad con nivel de impacto alto a través de otras instituciones gubernamentales.

- Mantener la documentación de la implementación del EGSI debidamente organizada.

- Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos.

- Informar al Comité de Seguridad de la Información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), así como las alertas que impidan su implementación.

- Previa la terminación de sus funciones el Oficial de Seguridad realizará la transferencia de la documentación e información de la que fue responsable al nuevo Oficial de Seguridad, en caso de ausencia, al Comité de Seguridad de la Información.

2.3.6 Planes de Acción

Una vez realizado el diagnóstico inicial de la institución y la evaluación realizada, se requiere implementar planes de acción con la finalidad que la institución pueda empezar a gestionar su propio programa, manteniendo un feedback contante cada que se vaya cumpliendo los hitos en los planes de acción.

Tabla 8. Planes de Acción - Dominio de Seguridad (ISO/IEC 27001.2013) Anexo A.

Planes de Acción - Dominio de Seguridad (ISO/IEC 27001.2013) Anexo A.	
A.5	Política De La Seguridad De La Información
A.6	Organización De La Seguridad De La Información
A.7	Seguridad En Los Recursos Humanos
A.8	Gestión De Activos
A.9	Control De Acceso
A.10	Criptografía
A.11	Seguridad Física Y Ambiental
A.12	Seguridad De Las Operaciones
A.13	Seguridad De Las Comunicaciones
A.14	Adquisición, Desarrollo Y Mantenimiento De Sistemas
A.15	Relaciones Con Proveedores
A.16	Gestión De Incidentes De Seguridad De La Información

A.17	Aspectos De Seguridad De La Información De La Gestión De La Continuidad De Negocio
A.18	Conformidad

3. CONCLUSIONES Y RECOMENDACIONES

3.1 CONCLUSIONES

En la actualizada la institución muestra un serio fallo de seguridad informática, ya que no cuenta con políticas en su mayoría en estado administrado, limitando la mejora continua, medición y control del proceso.

Según el análisis y las evaluaciones realizadas usando la ISO27001:2013 se evidencia que la institución no garantiza la seguridad de la información manejas en cada uno de sus servicios, ni la capacidad de responder ante algún incidente informático.

La clasificación de los activos de información en la institución a permitido a la institución establecer prioridades para la implementación del plan de mejoramiento propuesto, el valor de la información identificada es muy sensible para la institución, se ha tomado las medidas necesarias por mitigar el riesgo, haciendo que el Sistema de Gestión de Seguridad de la Información actual se fortalezca en la institución.

El plan de mejora desarrollada se adapta a las necesidades de la institución y posiciona sus mejoras para apoyar en su visión y misión institucionales, teniendo en cuenta el impacto en un sector sensible del espacio aéreo ecuatoriano ante un ataque a la ciberseguridad.

3.2 RECOMENDACIONES

Es relevante adquirir una cultura a las acciones y nociones que todos los funcionarios de la institución posean, deben conocer métodos para no ser blancos fáciles de un ciberataque, contando con los conocimientos necesarios para la protección de los datos de información.

La institución debe adoptar un análisis metodológico en el cual se identifique los activos de información más críticos evaluándolos periódicamente, haciendo que las vulnerabilidades encontradas entren a un tratamiento en el cual se implemente y se refuercen controles que ayuden a minimizar el riesgo.

El programa de mejora del SGSI adopta marcos de referencia estructurados el cual deben ser implementado a medida, con forme a la estructura institucional, permitiendo implementar buenas prácticas, sobre todos anteponiendo la formación del personal en temas de seguridad de la información, los cuales se encargado de que el sistema de gestión funcione correctamente.

4. REFERENCIAS

Excellence, I. (2019). *Seguridad de la Información*. Obtenido de https://www.pmg-ssi.com/norma-27001/

Mejía, J. C. (24 de Febrero de 2021). *UCE-DTIC*. Obtenido de https://uce-dtic.blogspot.com/2021/02/metodologia-magerit-analisis-y-gestion.html

MINTEL. (10 de Enero de 2010). Acuerdo Ministerial No.025-2019 Esquema Gubernamental de Seguridad de la Información - EGSI (versión 2.0). Quito, Pichincha, Ecuador.

Pozo, R. P. (6 de 6 de 2016). Elaboración de un Plan de Implementación de. Catalunya.

Salazar, L. (15 de Febrero de 2021). *pirami*. Obtenido de https://www.piranirisk.com/es/blog/que-es-el-apetito-de-riesgo#:~:text=El%20apetito%20al%20riesgo%2C%20es,para%20alcanzar%20sus%20objetivos%20estrat%C3%A9gicos.

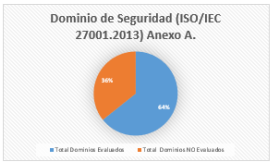
5. ANEXOS

Metodología de evaluación del SGSI para la Institución

El presente trabajo proporcionará los requisitos para establecer, implementar y mantener el mejoramiento contínuo del Esquema Gubernamental de Seguridad de la Información, en la Institución que pretende administrar el Sistema de Gestión de Seguridad, se basara en la Esquema Gubernamental de Seguridad de la Información (EGSI) normado por la ISO/IEC 27001:2013, la cual es una norma internacional que permitirá el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan, con el objetivo de brindar los lineamientos para que la institución inicien con la implementación del EGSI o la

La ISO/IEC 27001:2013, es una norma internacional emitida por la Organización Internacional de Normalización ISO. Esta norma fue publicada el 15 de octubre del año 2005 y posteriormente revisada el 25 de septiembre de 2013. Esta norma, se elaboró con el fin de conceder los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información.
Recuperado de: *Excellence, b. e. (02 de 02 de 2020). ISO27000.ES. Obtenido de https://www.pmg-ssi.com/norma-27001/*

	Dominio de Seguridad (ISO/IEC 27001.2013) Anexo A.	Presen	Observación
A.5	POLITICA DE LA SEGURIDAD DE LA INFORMACIÓN	SI	
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	SI	
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	NO	No se tiene información
A.8	GESTIÓN DE ACTIVOS	SI	
A.9	CONTROL DE ACCESO	SI	
A.10	CRIPTOGRAFIA	NO	No requiere este control
A.11	SEGURIDAD FISICA Y AMBIENTAL	NO	No se tiene información
A.12	SEGURIDAD EN LAS OPERACIONES	SI	
A.13	SEGURIDAD EN LAS COMUNICACIONES	SI	
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	SI	
A.15	RELACIONES CON PROVEEDORES	NO	No se tiene información
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	SI	
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	SI	
A.18	CUMPLIMIENTO	NO	No se tiene información
	Total Dominios	9	64%
	Total Dominios NO	5	36%



EVALUACIÓN

Mediante la recopilación de información en la Dirección General de Aviación Civil, en conjunto con el Oficial de Seguridad de la institución, se ha permitido evaluar 9 dominios de 14 que dicta la norma ISO/IEC 27001.2013 , los cuales se dividen en objetivos del control y su control especifico, dando una ponderación a cada objetivo de control referente a la situación actual siguiente:

1	Inicial	Se evidencia que existe un procedimiento sin la debida gestión, se lleva a cabo los procesos
2	Definido	El control se encuentra aplicado y documentado, el documento se encuentra debidamente
3	Administrado	El control documentado se encuentra legalizado bajo una mejora continua, medición y control
4	Optimizado	El control cumple con las directrices gubernamentales, teniendo una innovación del proceso y su

Numero de Controles Evaluados	Estado de Control Evaluado
28	Inicial
29	Definido
19	Administrado
0	Optimizado

Inicial
Definido
Administrado
Optimizado

ID	ISO27001:2013 - ANEXO A		Control	Nivel de cumplimiento del control	Valoración Actual
A.5	POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.	3	Administrado
			A.5.1.2. Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.	3	Administrado
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A.6.1. Organización Interna.	A.6.1.1. Seguridad de la Información Roles y Responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	4	Optimizado
			A.6.1.2. Separación de deberes. Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.	4	Optimizado
			A.6.1.3. Contacto con las autoridades. Se debe mantener contactos apropiados con las autoridades pertinentes.	2	Definido
			A.6.1.4. Contacto con grupos de interés especial. Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	1	Inicial
			A.6.1.5. Seguridad de la información en Gestión de Proyectos. La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto,	1	Inicial
		A.6.2. Dispositivos Móviles y Teletrabajo.	A.6.2.1. Política para dispositivos móviles. Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	1	Inicial
			A.6.2.2. Teletrabajo. Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	1	Inicial
			A.8.1.1. Inventario de Activos. Se deben identificar los activos asociados con información e instalaciones de procesamiento de		

A.8.	GESTIÓN DE ACTIVOS	A.8.1. Responsabilidad por los Activos.	A.8.1.1. Inventario de Activos. Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	3	Administrado
			A.8.1.2. Propiedad de los activos. Los activos mantenidos en el inventario deben ser propios.	3	Administrado
			A.8.1.3. Uso Aceptable de los Activos. Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	3	Administrado
			A.8.1.4. Devolución de Activos. Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	3	Administrado
		A.8.2. Clasificación de la Información.	A.8.2.1. Clasificación de la Información. La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	2	Definido
			A.8.2.2. Etiquetado de la Información. Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	2	Definido
			A.8.2.3. Manejo de Activos. Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	2	Definido
		A.8.3. Manejo de medios de soporte.	A.8.3.1. Gestión de medios de Soporte Removibles. Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	1	Inicial
			A.8.3.2. Disposición de los medios de soporte. Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.	2	Definido
			A.8.3.3. Transferencia de medios de soporte físicos. Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	2	Definido

A.9.	CONTROL DE ACCESO	A.9.1. Requisitos del Negocio para Control de Acceso.	A.9.1.1. Política de Control de Acceso. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	3	Administrado
			A.9.1.2. Acceso a redes y a servicios en red. Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	3	Administrado
		A.9.2. Gestión de Acceso de Usuarios.	A.9.2.1. Registro y cancelación del registro de usuarios. Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.	3	Administrado
			A.9.2.2. Suministro de acceso de usuarios. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	3	Administrado
			A.9.2.3. Gestión de derechos de acceso privilegiado. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	3	Administrado
			A.9.2.4. Gestión de información de autenticación secreta de usuarios. La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.	3	Administrado
			A.9.2.5. Revisión de los derechos de acceso de usuarios. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.	2	Definido
			A.9.2.6. Cancelación o ajuste de los derechos de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	3	Administrado
		A.9.3. Responsabilidades de los usuarios.	A.9.3.1.Uso de información secreta. Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	3	Administrado
		A.9.4. Control de Acceso a Sistemas y Aplicaciones.	A.9.4.1. Restricción de acceso a información. El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	1	Inicial
			A.9.4.2. Procedimiento de Conexión Segura. Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.	3	Administrado
			A.9.4.3. Sistema de Gestión de Contraseñas.los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	3	Administrado
			A.9.4.4. Uso de programas utilitarios privilegiados. Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	1	Inicial
			A.9.4.5. Control de Acceso a Códigos Fuente de Programas. Se debe restringir el acceso a códigos fuente de programas.	1	Inicial

A.12.	SEGURIDAD DE LAS OPERACIONES	A.12.1. Procedimientos operacionales y responsabilidades.	A.12.1.1. Procedimientos de operación documentados. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.	1	Inicial	1,8
			A.12.1.2. Gestión de Cambios. Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	2	Definido	
			A.12.1.3. Gestión de Capacidad. Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	2	Definido	
			A.12.1.4. Separación de los ambientes de desarrollo, pruebas y operación. Se deben separar los ambientes de desarrollo, pruebas y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.	2	Definido	
		A.12.2. Protección contra códigos maliciosos.	A.12.2.1. Controles contra códigos maliciosos. Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para protegerse contra códigos maliciosos.	2	Definido	2,0
		A.12.3. Copias de Respaldo.	A.12.3.1. Copias de respaldo de la información. Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordada.	3	Administrado	3,0
		A.12.4. Registro y Seguimiento.	A.12.4.1. Registro de eventos. Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	1	Inicial	1,0
			A.12.4.2. Protección de la información de registro. Las instalaciones y la información de registros deben protegerse contra alteración y acceso no autorizados.	1	Inicial	
			A.12.4.3. Registros del administrador y del operador. Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.	1	Inicial	
			A.12.4.4. Sincronización de relojes. Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	1	Inicial	
		A.12.5. Control de Software Operacional.	A.12.5.1. Instalación de software en sistemas operativos. Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	2	Definido	2,0
		A.12.6. Gestión de vulnerabilidad técnica.	A.12.6.1. Gestión de las vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	1	Inicial	1,0
			A.12.6.2. Restricciones sobre la instalación de Software. Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.	1	Inicial	
		A.12.7. Consideraciones sobre auditorías de sistemas de información.	A.12.7.1. Controles sobre auditorías de Sistemas de Información. Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	1	Inicial	1,0

A.13.	SEGURIDAD DE LAS COMUNICACIONES	A.13.1. Gestión de Seguridad de Redes.	A.13.1.1. Controles de redes. Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	2	Definido
			A.13.1.2. Seguridad de los servicios de red. Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	3	Administrado
			A.13.1.3. Separación en las redes. Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	2	Definido
		A.13.2. Transferencia de información.	A.13.2.1. Políticas y procedimientos de transferencia de información. Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todos los tipos de instalaciones de comunicaciones.	1	Inicial
			A.13.2.2. Acuerdos sobre transferencia de información. Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	1	Inicial
			A.13.2.3. Mensajería electrónica. Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.	1	Inicial
			A.13.2.4. Acuerdos de confidencialidad o de no divulgación. Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	3	Administrado
A.14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	A.14.1. Requisitos de seguridad de los sistemas de información.	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información. Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	1	Inicial
			A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas. La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	1	Inicial
			A.14.1.3. Protección de transacciones de servicios de aplicaciones. La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada.	1	Inicial
		A.14.2. Seguridad en los procesos de desarrollo y de soporte.	A.14.2.1. Política de desarrollo seguro. Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas al desarrollar dentro de la organización.	2	Definido
			A.14.2.2. Procedimientos de control de cambios en sistemas. Los cambios a los sistemas dentro del ciclo de vida de desarrollo de software y de sistemas al desarrollar dentro de la organización.	2	Definido
			A.14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones. Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacional.	2	Definido
			A.14.2.4. Restricciones sobre los cambios de paquetes de software. Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	2	Definido
			A.14.2.5. Principios de construcción de sistemas seguros. Se deben establecer, documentar y mantener principios para la arquitectura de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.	2	Definido
			A.14.2.6. Ambiente de desarrollo seguro. Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	2	Definido
			A.14.2.7. Desarrollo contratado externamente. La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.	2	Definido
			A.14.2.8. Pruebas de seguridad de sistemas. Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de seguridad.	2	Definido
			A.14.2.9. Pruebas de aceptación de sistemas. Para los nuevos sistemas de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de ensayo y criterios relacionados.	2	Definido
		A.14.3. Datos de ensayo.	A.14.3.1. Protección de datos de ensayo. Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	1	Inicial

A.16.	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información.	A.16.1.1. Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	2	Definido
			A.16.1.2. Informe de eventos de seguridad de la información. Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.	1	Inicial
			A.16.1.3. Informe de debilidades de seguridad de la información. Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	2	Definido
			A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Los eventos de seguridad de la información se deben evaluar y se debe decidir si van a clasificar como incidentes de seguridad de la información.	2	Definido
			A.16.1.5. Respuesta a incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	2	Definido
			A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	1	Inicial
			A.16.1.7. Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que puede servir como evidencia.	2	Definido
A.17.	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	A.17.1. Continuidad de seguridad de la información	A.17.1.1. Planificación de la continuidad de la seguridad de la información. La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	1	Inicial
			A.17.1.2. Implementación de la continuidad de la seguridad de la información. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	1	Inicial
			A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	1	Inicial
		A.17.2. Redundancias	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información. Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	2	Definido

	Descripción	Situacion Actual	Situacion Deseada
1	POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN	3	4
2	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2	3
3	GESTIÓN DE ACTIVOS	3	4
4	CONTROL DE ACCESO	3	4
5	SEGURIDAD DE LAS OPERACIONES	2	3
6	SEGURIDAD DE LAS COMUNICACIONES	2	3
7	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	2	3
8	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	2	3
9	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	2	3

Planes de acción

Ítem	Área responsable del control	Sección	Descripción del Control	Planes a accion
		1	**Políticas de Seguridad de la Información**	
		1.1	**Dirección de gestión de seguridad de la información**	
1		1.1.1	Políticas de Seguridad de la Información	La máxima debe dar seguimiento a la implementación de este Esquema Gubernamental de Seguridad de la Información (EGSI) en la institución.
2		1.1.2	Revisión de las políticas para la seguridad de la información	Para garantizar la vigencia de la política de seguridad de la información en la institución, esta debe ser revisada anualmente o cuando se produzcan cambios significativos a nivel operativo, legal, tecnológica, económico, entre otros; los cuales deben ser documentados y versionados.
		2	**Organización de la Seguridad de la Información**	
		2.2	**Dispositivos móviles y teletrabajo**	
9		2.2.1	Política de dispositivos móviles	Actualizar anualmente la Política de dispositivos móviles, con la finalidad de mantener la seguridad adecuadas para la protección y gestión de los riesgos generados por el uso de dispositivos móviles
10		2.2.2	Teletrabajo	Se debe Implementar una política y medidas de seguridad de apoyo, para proteger la información a la que se accede, procesa o almacena en ubicaciones destinadas a esta modalidad de trabajo para los funcionarios de la institución.
		5	**Control de acceso**	
		5.1	Requisitos institucionales para el control de acceso	
27		5.1.1	Política de control de acceso	Se debe implementar una Política de control de acceso con la finalidad de gestionar los accesos de los usuarios a los sistemas de información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados, definiendo las responsabilidades para identificar, gestionar y mantener perfiles de los custodios de información.
28		5.1.2	Acceso a redes y servicios de red	Se debe implementar una Política Acceso a redes y servicios de red, con la finalidad de Identificar y documentar los equipos que se encuentran en las redes debidamente autorizados, así mismo identificar usuarios debidamente autorizados para acceder a las redes y servicios de red a través de VPN, redes virtuales y redes inalámbricas entre otras.
		5.3	Responsabilidades del usuario	
35		5.3.1	Uso de la información confidencial para la autenticación	Se debe elaborar una política, implementarla y socializar a los funcionarios las responsabilidades del uso de las credenciales de acceso a la información y a los equipos informaticos puestos a su disposición
		5.4	Control de acceso a sistemas y aplicaciones	
36		5.4.1	Restricción del acceso a la información	Se debe elaborar una política para restringir el acceso de los usuarios a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.
37		5.4.2	Procedimientos seguros de inicio de sesión	Se debe actualizar anualmente un procedimiento seguro de inicio de sesión cuando se requiera una autenticación robusta, para controlar el acceso a los sistemas y aplicaciones institucionales por ejemplo medios criptográficos, tarjetas inteligentes, dispositivos hardware.
38		5.4.3	Sistema de gestión de contraseñas	Se debe elaborar una política, implementarla y socializar a los funcionarios las responsabilidades del uso Sistema de gestión de contraseñas
39		5.4.4	Uso de herramientas de administración de sistemas	Se debe elaborar una política, implementarla y socializar a los funcionarios el Uso de herramientas de administración de sistemas
40		5.4.5	Control de acceso al código fuente del programa	Se debe elaborar una política, implementarla y socializar a los funcionarios las responsabilidades Control de acceso al código fuente del programa
		7	**Seguridad física y del entorno**	
		8.2	Protección contra un malware	
62		8.2.1	Controles contra malware	Se debe actualizar la Resolucion 323 – 2012"Reglamento para el uso y control de los recursos informaticos y comunicaciones de la institución, con la finalidad de prohibir el uso de software no autorizado por la institución.
		8.3	Copias de seguridad	
63		8.3.1	Copias de seguridad de la información	Se debe implemetra una politica Copias de seguridad de la información con la finalidad de mantener los respaldados y puedan ser recuperables en el momento que se lo requiera.
		8.4	Registro y monitoreo	
64		8.4.1	Registro de eventos	Se debe Implementar un procedimiento para registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.
65		8.4.2	Protección de los registros de información	Elaborar un procedimiento para proteger contra posibles alteraciones y accesos no autorizados la información de los registros
66		8.4.3	Registros de administración y operación	Elaborar bitácoras para el registrar, proteger y revisar regularmente de acuerdo a las necesidades de la institución; las actividades del administrador y del operador del sistema
67		8.4.4	Sincronización de relojes	Mantener anualmente actualizado el Manual_Administración_del_servicio_AD
		8.5	Control del software en producción	

68		8.5.1	Instalación del software en sistemas en producción	Mantener actualizado el procedimientos para controlar la instalación adecuada de software en los sistemas en producción
		8.6	Gestión de la vulnerabilidad técnica	
69		8.6.1	Gestión de las vulnerabilidades técnicas	Elaborar e Implementar una política de monitoreo continuo sobre los sistemas en producción, detectar vulnerabilidades técnicas, adoptar las medidas necesarias para afrontar el riesgo asociado
70		8.6.2	Restricciones en la instalación de software	Mantener anualmente actualizado política de Restricciones en la instalación de software que rija la instalación de software por parte de los usuarios de la institución
		8.7	Consideraciones sobre la auditoría de sistemas de información	
71		8.7.1	Controles de auditoría de sistemas de información	Se debe Planificar y acordar los requisitos y las actividades de auditoria que involucran la verificación de los sistemas en producción con el objetivo de minimizar las interrupciones en los procesos relacionados con la institución.
		9	**Seguridad en las comunicaciones**	
		9.1	Gestión de la seguridad de redes	
72		9.1.1	Controles de red	
73		9.1.2	Seguridad de los servicios de red	Identificar e incluir en los acuerdos de servicio los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente si estos servicios se entregan de manera interna o están externalizados. (SLA´s)
74		9.1.3	Separación en las redes	Documentar pediodicamente la segregación de redes y mantener un control de las IP´s de cada segmento en la Dirección General de Aviación Civil - Matriz, en cada cambio o actualización que se genere.
		9.2	Transferencia de información	
75		9.2.1	Políticas y procedimientos de transferencia de información	Elaborar implementar una política, procedimiento y control formales que protejan la transferencia de información que viaja a través del uso de todo tipo de recursos de comunicación o se debe actualizar la Resolucion 329 - 2012"Reglamento para el uso y control de los recursos informaticos y comunicaciones de la institución
76		9.2.2	Acuerdos de transferencia de información	Se debe elaborar e implementar acuerdos de transferencia de información y softw are segura, entre la institución y terceros
77		9.2.3	Mensajería electrónica	Establecer una política y procedimiento necesario, en la información de mensajería electrónica, debidamente reglamentada de acuerdo a la norma legal vigente o se debe actualizar la Resolucion 329 - 2012"Reglamento para el uso y control de los recursos informaticos y comunicaciones de la institución
78		9.2.4	Acuerdos de confidencialidad o no revelación	Mantener actualizado el CUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN PARA LOS FUNCIONARIOS, SERVIDORES Y TRABAJADORES DE LA DGAC y llevar un control de los usuarios que aceptan el

		10	**Adquisición, desarrollo y mantenimiento de los sistemas**	
		10.1	Requisitos de seguridad de los sistemas de información	
79		10.1.1	Análisis de requisitos y especificaciones de seguridad de la información	se debe actualizar la Resolucion 329 - 2012"Reglamento para el uso y control de los recursos informaticos y comunicaciones de la institución
80		10.1.2	Asegurar los servicios de aplicaciones en redes públicas	se debe actualizar la Resolucion 329 - 2012"Reglamento para el uso y control de los recursos informaticos y comunicaciones de la institución
81		10.1.3	Controles de transacciones en línea	
		10.2	Seguridad en el desarrollo y en los procesos de soporte	
82		10.2.1	Política de desarrollo seguro	Mantener actuailizada y socializar la Política de desarrollo seguro, con la finalidad de mantener el desarrollo de aplicaciones y sistemas en la institución de forma segura.
83		10.2.2	Procedimientos de control de cambios en sistemas	Mantener actuailizada Procedimientos de control de cambios en sistemas con la finalidad de llevar un control a los cambios a lo largo del ciclo de vida del desarrollo del softw are.
84		10.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Mantener actuailizada Procedimientos de control de cambios en sistemas con la finalidad de Evitar las modificaciones en el softw are suministrado o adquirido a terceros por la institución, limitarse a cambios realmente necesarios; considerar un control estricto sobre los cambios
85		10.2.4	Restricciones a los cambios en los paquetes de softw are	
		11	**Relaciones con proveedores**	
		11.1	Seguridad de la información en relación con los proveedores	
92		11.1.1	Política de seguridad de la información en las relaciones con los proveedores	Actualizar anualmente la Política Política de seguridad de la información en las relaciones con los proveedores.
93		11.1.2	Requisitos de seguridad en contratos con terceros	Mantener en archivo digital el acuerdo de confidencialidad legalizado con la finalidad de obterne informacion en posibles asuntos legales que se viera afectada la informacion.
94		11.1.3	Cadena de suministro de tecnologías de la información y de las comunicaciones	Se debe mejorar los acuerdos con proveedores, solicitando requisitos adicinales para enfrentar los riesgos de seguridad de la información que tienen relación con las TIC's.
		11.2	Gestión de la provisión de servicios del proveedor	
95		11.2.1	Monitoreo y revisión de los servicios de proveedores	Se debe desarrolar una política para que la institución pueda monitorear, evaluar y auditar continuamente la provisión de servicios del proveedor
96		11.2.2	Gestión de cambios en los servicios de proveedores	Se debe desarrolar una política para la gestionar los cambios en la provisión de servicios, mantenimiento, mejora de políticas, procedimientos y controles de seguridad de la información; considerando la criticidad de los procesos y sistemas de la institución afectados, así como la revisión y reapreciación de los riesgos, de acuerdo a la norma legal vigente

		12	**Gestión de incidentes de seguridad de la información**	
		12.1	Gestión de los incidentes de seguridad de la información y mejoras	
97		12.1.1	Responsabilidades y procedimientos	Se debe desarrollar una política para la Gestión de incidentes de seguridad de la información, para Establecer formalmente responsabilidades y procedimientos para asegurar una respuesta rápida, efectiva y acorde a los incidentes de seguridad de la información que pueden ocurrir en la institución
98		12.1.2	Reporte de los eventos de seguridad de la información	
99		12.1.3	Reporte de debilidades de seguridad de la información	
100		12.1.4	Apreciación y decisión sobre los eventos de seguridad de la información	
101		12.1.5	Respuesta a incidentes de seguridad de la información	
102		12.1.6	Aprendizaje de los incidentes de seguridad de la información	
103		12.1.7	Recopilación de evidencias	

Apetito al riesgo

Impacto	Aversión	Neutral	Agresivo
Perdidas Financieras para el Estado Ecuatoriano	X		
Interacción de las operaciones aeronauticas parciales y/o totales	X		
Demandas Judiciales / afectación Legal (Nacional y/o Internacional)		X	X
Perdida / Degradación de la Imagen Institucional	X	X	
Sumarios administrativos (Despido de personal)			X

Tipología de Impacto - Nivel de Riesgo	Insignificante	Menor	Moderado	Mayor	Catastrofico
Perdidas Financieras para el Estado Ecuatoriano	No aplica para la institución	Perdidas menores del 5% de los valores netos por el servicios de trasporte aéreo	Perdidas mayores al 5 % y menores al 10 % de los valores netos por el servicios de trasporte aéreo	Perdidas mayores al 10 % y menores al 15 % de los valores netos por el servicios de trasporte aéreo	Perdidas mayores al 20 % de los valores netos por el servicios de trasporte aéreo
Interupción de las operaciones parciales y/o totales	No aplica para la institución	No apliva para la institución	Perdida del servicio de 0 a 5 minutos	Perdida del servicio de 5 a 15 minutos	Perdida del servicio de Mayor a 15 minutos
Demandas Judiciales / afectación Legal (Nacional y/o Internacional)	No aplica para la institución	Reclamos por parte del usuario por la no disponibilidad de los servicios	Sanciones legales por la no disponibilidad de los servicios (Nivel Nacional)	Sanciones legales por la no disponibilidad de los servicios (Nivel Internacional)	Sanciones legales por la no disponibilidad de los servicios (Estado Ecuatoriano)
Perdida / Degradación de la Imagen Institucional	No aplica para la institución	No apliva para la institución	Pérdida de confianza por partes de los usuarios que utilizan los servicios	Pérdida de confianza de por parte de las aerolíneas aéreas que utiliza los servicios	Pérdida de confianza por partes del Estado Ecuatoriano
Sumarios administrativos (Despido de funcionarios técnicos)	No aplica para la institución	No apliva para la institución	(1) un Funcionario técnico al año	(2) dos funcionarios técnico al año	(3) tres funcionarios técnicos al año

CONFIDENCIALIDAD	CRITERIO	Valoración
Alto	La divulgación no autorizada de la información tiene un efecto crítico para la institución Ej, Divulgación de información confidencial o sensible.	3
Medio	La divulgación no autorizada de la información tiene un efecto limitado para la institución Ej. Divulgación de información de uso interno	2
Bajo	La divulgación de la información no tiene ningún efecto para la institución Ej. Divulgación de información pública.	1

INTEGRIDAD	CRITERIO	Valoración
Alto	La destrucción o modificación no autorizada de la Información tiene un efecto severo para la institución	3
Medio	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución	2
Bajo	La destrucción o modificación de la información tiene un efecto leve para la institución	1

DISPONIBILIDAD	CRITERIO	Valoración
Alto	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución	3
Medio	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución	2
Bajo	La interrupción al acceso de la información o los sistemas. tienen un efecto mínimo para la institución	1

PRIVACIDAD	CRITERIO	Valoración
Alto	La vulneración a los acceso restringidos de la información o los sistemas tienen un efecto severo para la institución	3
Medio	La vulneración a los acceso restringidos de la información o los sistemas tienen un efecto considerable para la institución	2
Bajo	La vulneración a los acceso restringidos de la información o los sistemas. tienen un efecto mínimo para la institución	1

Modulador del Activo Critico		
valor	Criterio	Descripción
3	Daño Grave	Critico
2	Daño Importante	Medio
1	Daño Menor	Bajo

Entidades y Tipos de Información

Entidad	Nombre del tipo de informacion	Confidencialidad						
		Perdidas Financieras para el Estado Ecuatorian	Interupción de las operaciones parciales	Demandas Judiciales / afectación Legal	Perdida / Degradación de la Imagen Institucion	Sumarios administrativos (Despido de	Evaluación de Confidencialidad	
Pilotar Aéreo	Información General del Pilato	1	1	2	3	1	1,6	
	Información de licencia del pilato	1	1	2	3	1	1,6	
	Información de documentación habilitante del pilato	2	1	2	1	2	1,6	
Campañías Aéreas	Información general de Campañías aéreas (nacional o extranjera)	1	1	2	1	2	1,4	
	Información del representante técnica de Campañías aéreas	1	1	2	2	2	1,6	
	Información Legal de las campañías aéreas	1	2	3	2	2	2	
	Información general de las aeronaves de las Campañías Aéreas	3	2	1	1	1	1,6	
	Información técnica de las aeronaves de las Campañías Aéreas	1	1	1	1	1	1	
	Información de validación de certificaciones de las aeronaves de las Campañías Aéreas	2	3	2	2	3	2,4	
	Información de planes de vuelo de las aeronaves de las Campañías Aéreas	3	3	3	3	3	3	
	Información meteorológica de la Campañías Aéreas	2	2	3	3	2	2,4	

Entidad	Nombre del tipo de informacion	Confidencialidad					
		Perdidas Financieras para el Estado Ecuatorian	Interupción de las operaciones parciales	Demandas Judiciales / afectación Legal	Perdida / Degradación de la Imagen Institucion	Sumarios administrativos (Despido de	Evaluación de Confidencialidad
Funcionarios	Información general del funcionario	1	1	1	1	1	1
	Información de datos físicos del funcionario	1	1	2	2	2	1,6
	Información Médica del funcionario	1	1	2	2	2	1,6
	Información familiar del funcionario	1	1	2	2	2	1,6
	Información financiera del funcionario	2	2	3	2	2	2,2
Proveedores	Información de contacto del proveedor	1	1	2	2	1	1,4
	Información Legal del Proveedor	1	1	2	2	1	1,4
	Información Financiera del proveedor	1	1	2	2	1	1,4

Entidad	Nombre del tipo de informacion	Integridad					
		Perdidas Financieras para el Estado Ecuatorian	Interupción de las operaciones parciales	Demandas Judiciales / afectación Legal	Perdida / Degradación de la Imagen Institucion	Sumarios administrativos (Despido de	Evaluación de Integridad
Pilotos Aéreos	Información General del Pilato	2	2	2	2	2	2
	Información de licencia del pilato	2	2	3	2	2	2,2
	Información de documentación habilitante del pilato	1	2	1	2	3	1,8
Compañías Aéreas	Información general de Compañías aéreas (nacionales extranjera)	1	2	2	2	1	1,6
	Información del representante técnica de Compañías aéreas	1	2	2	2	1	1,6
	Información Legal de las compañías aéreas	1	2	2	2	1	1,6
	Información general de las aeronaves de las Compañías Aéreas	1	2	2	2	1	1,6
	Información técnica de las aeronaves de las Compañías Aéreas	1	2	2	2	1	1,6
	Información de validación de certificaciones de las aeronaves de las Compañías Aéreas	1	3	3	2	3	2,4
	Información de planes de vuelo de las aeronaves de las Compañías Aéreas	3	3	3	3	3	3
	Información meteorológica de la Compañías Aéreas	3	3	3	3	3	3

Entidad	Nombre del tipo de informacion	Integridad					
		Perdidas Financieras para el Estado Ecuatorian	Interupción de las operaciones parciales	Demandas Judiciales / afectación Legal	Perdida / Degradación de la Imagen Institucion	Sumarios administrativos (Despido de	Evaluación de Integridad
Funcionarios	Información general del funcionario	1	2	2	3	1	1,8
	Información de datos físicos del funcionario	1	2	2	2	1	1,6
	Información Médica del funcionario	1	2	2	3	1	1,8
	Información familiar del funcionario	1	2	2	2	1	1,6
	Información financiera del funcionario	2	3	2	1	2	2
Proveedores	Información de contacto del proveedor	1	2	2	2	1	1,6
	Información Legal del Proveedor	1	2	2	3	1	1,8
	Información Financiera del proveedor	1	2	2	2	1	1,6

Entidad	Nombre del tipo de informacion	Disponibilidad					
		Perdidas Financieras para el Estado Ecuatorian	Interupción de las operaciones parciales	Demandas Judiciales / afectación Legal	Perdida / Degradación de la Imagen Institucion	Sumarios administrativos (Despido de	Evaluación de Disponibilidad
Pilotos Aéreos	Información General del Pilato	1	2	2	2	1	1,6
	Información de licencia del pilato	1	2	2	2	1	1,6
	Información de documentación habilitante del pilato	2	2	2	2	2	2
Compañías Aéreas	Información general de Compañías aéreas (nacionales extranjera)	1	2	2	1	2	1,6
	Información del representante técnica de Compañías aéreas	1	1	2	1	1	1,2
	Información Legal de las compañías aéreas	1	1	2	1	1	1,2
	Información general de las aeronaves de las Compañías Aéreas	1	3	3	2	2	2,2
	Información técnica de las aeronaves de las Compañías Aéreas	1	3	3	2	2	2,2
	Información de validación de certificaciones de las aeronaves de las Compañías Aéreas	2	2	1	3	2	2
	Información de planes de vuelo de las aeronaves de las Compañías Aéreas	3	3	3	3	3	3
	Información meteorológica de la Compañías Aéreas	3	3	3	3	3	3

Entidad	Nombre del tipo de informacion	Disponibilidad					
		Perdidas Financieras para el Estado Ecuatorian	Interupción de las operaciones parciales	Demandas Judiciales / afectación Legal	Perdida / Degradación de la Imagen Institucion	Sumarios administrativos (Despido de	Evaluación de Disponibilidad
Funcionarios	Información general del funcionario	1	1	2	2	2	1,6
	Información de datos físicos del funcionario	1	1	2	2	2	1,6
	Información Médica del funcionario	1	1	2	2	2	1,6
	Información familiar del funcionario	1	1	2	2	2	1,6
	Información financiera del funcionario	1	3	3	2	2	2,2
Proveedores	Información de contacto del proveedor	1	1	1	1	1	1
	Información Legal del Proveedor	1	1	1	1	1	1
	Información Financiera del proveedor	1	1	1	1	1	1

Entidad	Nombre del tipo de informacion	Privacidad				
		Interupción de las operaciones parciales	Demandas Judiciales / afectación Legal	Perdida / Degradación de la Imagen Institucion	Sumarios administrativos (Despido de	Evaluación de Privacidad
Pilotos Aéreos	Información General del Pilato	1	2	2	1	1,4
	Información de licencia del pilato	1	2	2	1	1,4
	Información de documentación habilitante del pilato	2	1	2	2	1,6
Compañías Aéreas	Información general de Compañías aéreas (nacionales extranjera)	1	2	2	1	1,4
	Información del representante técnica de Compañías aéreas	1	2	2	1	1,4
	Información Legal de las compañías aéreas	1	2	2	1	1,4
	Información general de las aeronaves de las Compañías Aéreas	1	3	3	2	2
	Información técnica de las aeronaves de las Compañías Aéreas	1	3	3	2	2
	Información de validación de certificaciones de las aeronaves de las Compañías Aéreas	1	3	3	2	2
	Información de planes de vuelo de las aeronaves de las Compañías Aéreas	2	3	3	3	2,6
	Información meteorológica de la Compañías Aéreas	2	2	3	3	2,4

Entidad	Nombre del tipo de informacion	Privacidad				
		Interupción de las operaciones parciales	Demandas Judiciales / afectación Legal	Perdida / Degradación de la Imagen Institucion	Sumarios administrativos (Despido de	Evaluación de Privacidad
Funcionarios	Información general del funcionario	1	1	1	1	1
	Información de datos físicos del funcionario	1	2	2	2	1,6
	Información Médica del funcionario	1	2	2	2	1,6
	Información familiar del funcionario	1	1	1	2	1,2
	Información financiera del funcionario	2	2	2	1	1,6
Proveedores	Información de contacto del proveedor	1	1	1	1	1
	Información Legal del Proveedor	1	2	2	2	1,6
	Información Financiera del proveedor	1	2	2	1	1,4

Entidad	Nombre del tipo de informacion	Evaluación de Confidencialidad	Evaluación de Integridad	Evaluación de Disponibilidad	Evaluación de Privacidad	Nivel de Aceptación
Pilotos Aéreos	Información General del Pilato	Menor	Moderado	Menor	Menor	Aceptable
	Información de licencia del pilato	Menor	Mayor	Menor	Menor	Aceptable
	Información de documentación habilitante del pilato	Menor	Moderado	Moderado	Menor	Aceptable
Campañías Aéreas	Información general de Campañías aéreas (nacional o extranjera)	Menor	Menor	Menor	Menor	Aceptable
	Información del representante técnica de Campañías aéreas	Menor	Menor	Insignificante	Menor	Aceptable
	Información Legal de las campañías aéreas	Moderado	Menor	Insignificante	Menor	Aceptable
	Información general de las aeronaves de las Campañías Aéreas	Menor	Menor	Mayor	Moderado	Aceptable
	Información técnica de las aeronaves de las Campañías Aéreas	Insignificante	Menor	Mayor	Moderado	Aceptable
	Información de validación de certificaciones de las aeronaves de las Campañías Aéreas	Mayor	Mayor	Moderado	Moderado	Aceptable
	Información de planes de vuelo de las aeronaves de las Campañías Aéreas	Catastrofico	Catastrofico	Catastrofico	Catastrofico	Catastrofico
	Información meteorológica de la Campañías Aéreas	Mayor	Catastrofico	Catastrofico	Mayor	Catastrofico

Entidad	Nombre del tipo de informacion	Evaluación de Confidencialidad	Evaluación de Integridad	Evaluación de Disponibilidad	Evaluación de Privacidad	Nivel de Aceptación
Funcionarios	Información general del funcionario	Insignificante	Moderado	Menor	Insignificante	Aceptable
	Información de datos físicos del funcionario	Menor	Menor	Menor	Menor	Aceptable
	Información Médica del funcionario	Menor	Moderado	Menor	Menor	Aceptable
	Información familiar del funcionario	Menor	Menor	Menor	Insignificante	Aceptable
	Información financiera del funcionario	Mayor	Moderado	Mayor	Menor	Aceptable
Proveedores	Información de contacto del proveedor	Menor	Menor	Insignificante	Insignificante	Aceptable
	Información Legal del Proveedor	Menor	Moderado	Insignificante	Menor	Aceptable
	Información Financiera del proveedor	Menor	Menor	Insignificante	Menor	Aceptable

Activo críticos

Modulador del Activo Critico		
valor	Criterio	Descripción
3	Daño Grave	Critico
2	Daño Importante	Medio
1	Daño Menor	Bajo

Entidad	Nombre del tipo de informacion	Nivel de criticidad	Activo de Información	Componente	Evaluación	Calificación
Pilotos Aéreos	Información General del Piloto	Aceptable	sistema_(SIPA) Sistema de Información del Personal Aeronautico	Base de Datos	3	Critico
	Información de licencia del piloto	Aceptable		web service	2	Medio
	Información de documentación habilitante del piloto	Aceptable		Sistema Operativo	1	Bajo
Compañías Aéreas	Información general de Compañías aéreas (nacional o extranjera)	Aceptable	Servidor_Sistema_Integrado (CORE)	DB2	3	Critico
	Información del representante técnico de Compañías aéreas	Aceptable		DB2	2	Medio
	Información Legal de las compañías aéreas	Aceptable		DB2	3	Critico
	Información general de las aeronaves de las Compañías Aéreas	Aceptable		DB2	1	Bajo
	Información técnica de las aeronaves de las Compañías Aéreas	Aceptable		DB2	2	Medio
	Información de validación de certificaciones de las aeronaves de las Compañías Aéreas	Aceptable		DB2	2	Medio
	Información de planes de vuelo de las aeronaves de las Compañías Aéreas	Catastrofico	sistema_(IFIS) Internet informatión flight service	Base de Datos	3	Critico
	Información meteorológica de la Compañías Aéreas	Catastrofico		web service	3	Critico
Funcionarios	Información general del funcionario	Aceptable	Carpeta_compartida	Sistema Operativo	2	Medio
	Información de datos físicos del funcionario	Aceptable		Servidor físico	2	Medio
	Información Médica del funcionario	Aceptable		File Server	1	Bajo
	Información familiar del funcionario	Aceptable			2	Medio
	Información financiera del funcionario	Aceptable			1	Bajo
Proveedores	Información de contacto del proveedor	Aceptable	Carpeta_compartida	Sistema Operativo	1	Bajo
	Información Legal del Proveedor	Aceptable			1	Bajo
	Información Financiera del proveedor	Aceptable			2	Medio