Diseño del Sistema de Gestión de Seguridad de la Información para el Instituto de Investigaciones Ambientales del Pacífico

JIMMY GEOVANNY LLOREDA MOSQUERA

Propuesta de trabajo de grado presentado como requisito parcial para optar al título de Magíster en seguridad de la información

Director:

PhD (c) Mauricio Mejía Lobo

Línea de Investigación
Sistemas de Gestión de Seguridad de la información
Grupo de Investigación y Desarrollo en Informática y Telecomunicaciones
Universidad de Manizales
Facultad de Ciencias e Ingeniería
Maestría en Seguridad de la Información
Manizales, 2024

Resumen

El propósito de este trabajo de investigación fue desarrollar un Sistema de Gestión de Seguridad de la Información específicamente diseñado para el Instituto de Investigaciones Ambientales del Pacífico. Para este fin, se consideraron las directrices establecidas en el estándar ISO 27001:2022 y el Modelo de Seguridad y Privacidad de la Información del MinTIC. Se hizo un análisis del estado inicial de la protección de la información en la institución, para elaborar una política de seguridad de la información acorde con la misión del Instituto. Se aplicó una metodología para la identificación de los activos de información y sus respectivos riesgos, aprovechando diversas herramientas, controles y procesos para obtener la declaración de aplicabilidad dentro de la entidad. Como resultado, se obtuvo una línea base que describe la situación de la entidad en términos de cumplimiento de los estándares de seguridad con respecto a los activos de información identificados, clasificados y evaluados. Además, se formuló una política de seguridad que ha sido adoptada por la entidad y que contribuye a mitigar los riesgos, amenazas y vulnerabilidades identificados dentro del Instituto. Esto resalta la urgencia de implementar lo antes posible las medidas y recomendaciones derivadas de los estándares internacionales y del Modelo de Seguridad y Privacidad de la Información (MSPI), que requiere una actualización, especialmente en lo referente al Anexo A de la ISO 27001:2022.

Palabras clave: Sistema de Gestión de Seguridad de la Información, Modelo de Seguridad y Privacidad de la Información, Activos de Información, Estándares ISO.

Abstract

The purpose of this research work was to develop an Information Security Management System specifically designed for the Pacific Environmental Research Institute. For this purpose, the guidelines established in the ISO 27001:2022 standard and the MinTIC Information Security and Privacy Model were considered. An analysis of the initial state of information protection in the institution was conducted, with the objective of developing an information security policy consistent with the Institute's mission. A methodology was applied to identify information assets and their respective risks, taking advantage of various tools, controls, and processes to obtain the statement of applicability within the entity. As a result, a baseline was obtained that describes the entity's situation in terms of compliance with security standards with respect to the information assets identified, classified, and evaluated. In addition, a security policy was formulated that has been adopted by the entity and that contributes to mitigating the risks, threats and vulnerabilities identified within the Institute. This highlights the urgency of implementing as soon as possible the measures and recommendations derived from international standards and the Information Security and Privacy Model (MSPI), which requires an update, especially regarding Annex A of ISO 27001:2022.

Keywords: Information Security Management System, Information Security and Privacy Model, Information Assets, ISO Standards.

Contenido

Pág.

Índice de figuras

Pág.

Índice de tablas

Pág.

Índice de Anexos

Lista de abreviaturas

Abreviatura	Término
IIAP	Instituto de Investigaciones Ambientales del Pacífico.
ISO	International Organization for Standardization
ITA	Índice de Transparencia y Acceso a la información
MinTIC	Ministerio de tecnologías de la Información y las Comunicaciones de Colombia.
MSPI	Modelo de Seguridad y Privacidad de la Información.
PHVA	Planear, Hacer, Verificar, Actuar
POA	Plan Operativo Anual
SGC	Sistema de Gestión de la Calidad
SGSI	Sistema de Gestión de Seguridad de la Información.
SINA	Sistema Nacional Ambiental
TI	Tecnología de la Información

INTRODUCCIÓN

El Instituto de Investigaciones Ambientales del Pacífico tiene como rol misional la producción de información y conocimiento del Chocó Biogeográfico, con el fin de fundamentar la toma de decisiones y las políticas públicas nacionales, regionales y locales en materia ambiental y de desarrollo sostenible.

La entidad genera información en materia Ambiental, ecosistémica, sistemas productivos, Sociocultural, ordenamiento territorial entre otros, la cual se ve reflejada en sus cuatros componentes principales de Investigación (Componentes Ambiental, Ecosistémico y productivo) y su laboratorio de datos.

En la tabla 1 se presenta un resumen del número proyectos realizados por el IIAP en el marco de su plan anual de inversión POA entre los años 2016 a 2023 y el valor económico de estos:

Tabla 1 No de Proyectos realizados por el IIAP 2016 - 2023

RESUMEN DEL NÚMERO DE PROYECTOS REALIZADOS POA IIAP 2016 - 2023			
ÍTEM	CANTIDAD DE PROYECTOS	VALOR TOTAL	AÑO
1	19	$ 2.430.599.172	2016
2	24	$ 5.092.400.000	2017
3	18	$ 3.430.637.858	2018
4	23	$ 4.923.086.057	2019
5	28	$ 5.570.486.338	2020
6	28	$ 10.570.486.338	2021
7	28	$ 4.625.200.928	2022
8	20	$ 5.000.000.000	2023

Nota. Elaboración propia, fuente base de datos proyectos de inversión del IIAP 2016-2023

El resultado de los diferentes informes de estos proyectos, actualmente no se centraliza en una instancia oficial, por lo que su disposición final es dispersa, lo que dificulta su custodia, integralidad y consulta.

En la tabla 2 se puede observar el consolidado de las investigaciones realizadas por el IIAP en toda su área de influencia, que encuentra en territorios colectivos de comunidades negras y resguardos indígenas, son un total de 638 investigaciones, que son el resultado de concertación y trabajo mancomunado con las comunidades y la articulación diferentes entidades del orden Internacional, nacional y regional, así como la sociedad civil en general.

Tabla 2 Consolidado de investigaciones 2007 -2022

CONSOLIDADO INVESTIGACIONES REALIZADAS POR EL IIAP ÁREA DE INFLUENCIA 2007 - 2022	
DEPARTAMENTO O ZONA	CANTIDAD
Antioquia	14
Antioquia – Chocó	5
Antioquia-Chocó-valle del cauca-cauca	1
Antioquia-Risaralda	1
Antioquia-valle del cauca-Nariño	1
Atrato	1
Cauca	67
Cauca – Chocó	4
Cauca – Nariño	1
Cauca - valle del cauca – Chocó	2
Cauca y valle del cauca	1
Cauca-Nariño	1
Cauca-valle del cauca	2
Chicó	1
Chocó	298
Chocó	1
Chocó – Antioquia	3
Chocó - cauca - valle del cauca	1
Chocó - valle del cauca	1
Chocó biogeográfico	2
Chocó -cauca	1

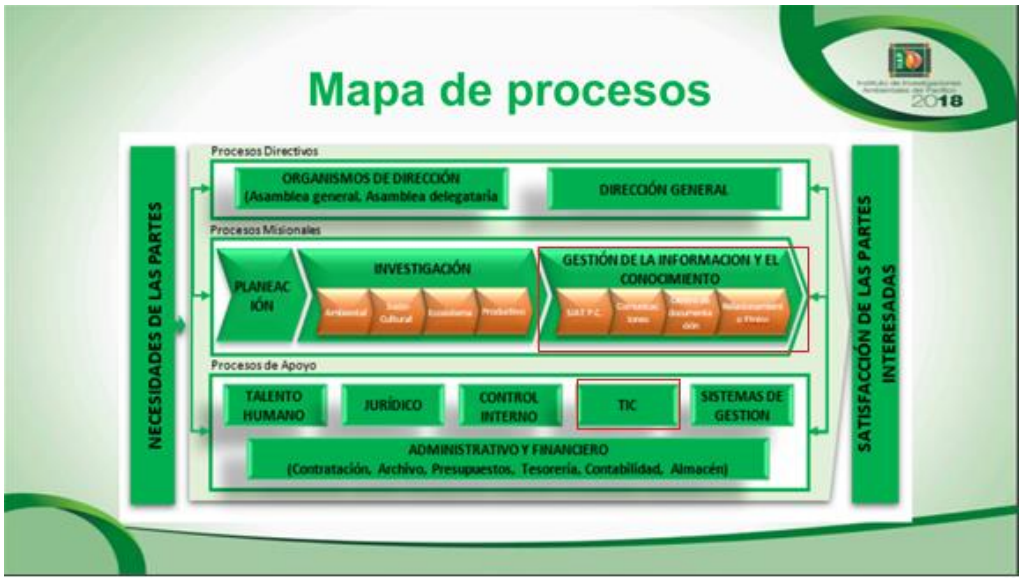
CONSOLIDADO INVESTIGACIONES REALIZADAS POR EL IIAP ÁREA DE INFLUENCIA 2007 - 2022	
DEPARTAMENTO O ZONA	CANTIDAD
Chocó, valle del Cauca – Nariño	1
Chocó-cauca-Nariño-valle del cauca	1
Chocó-cauca-valle del cauca	1
Chocó-valle del cauca	
Chocó-valle-cauca	1
Córdoba	16
Córdoba – Antioquia	1
Córdoba - valle del cauca - cauca - Risaralda	1
Córdoba	1
Guajira	1
Nariño	56
Risaralda	18
Risaralda – Chocó	1
Risaralda y Chocó	1
Valle del cauca	37
Valle del cauca - Chocó – cauca	1
Valle del cauca - Chocó – Risaralda	1
Valle del cauca – Nariño	1
Valle del cauca - Nariño – cauca	1
Valle del cauca-cauca-Chocó	3
Chocó biogeográfico	85
TOTAL GENERAL	**638**

1. Planteamiento del problema de investigación y su justificación

Aunque el Instituto de Investigaciones Ambientales del Pacífico tiene un sistema de gestión de calidad basado en buenas prácticas, caracterizado por procesos directivos, misiones y apoyo, como se muestra en la figura 1, mapa de procesos, no son suficientes para contrarrestar los riesgos que podrían afectar la entidad, en temas relacionados con la protección de la integralidad de la información, lo que hace relevante tener políticas claras y definidas respecto de la seguridad y privacidad de la información, para evitar incidentes que afecten su confidencialidad, disponibilidad o integridad.

Figura 1

Mapa de proceso SGC del IIAP



Fuente: Figura tomada del SGC del IIAP.

Teniendo presente que por su rol misional, el resultado de las diferentes investigaciones realizadas por el IIAP es su bien principal, la entidad debe propender por determinar los estándares relacionados a con la seguridad de la información que se acomoden de manera acorde a su funcionalidad, por ello y teniendo en cuenta que para el año 2021 el Ministerio de las Tecnologías y la Información (MinTIC), estableció unos Lineamentos y estándares enfocados a generar estrategias de seguridad digital que sean capaces de brindar garantías en este sentido, adopto el Modelo de Seguridad y Privacidad de la Información (MSPI), como habilitador de la política de Gobierno Digital (MinTIC, 2021). Cabe resaltar que la entidad al no tener una implementación de medidas como las del modelo, se ve expuestas a malas prácticas o taques a sus activos de información por personal interno o externo, lo que puede conllevar consecuencias negativas tanto legales como operativos. Adicionalmente por tratarse de una entidad de carácter

mixto, se asume la importancia de implementar y dar cumplimiento a las normas y procedimientos establecidos para las Organizaciones públicas del país, definidas por las leyes, los ministerios y en general por los entes gubernamentales de seguimiento y control.

Así las cosas, se hace necesario diseñar y planificar la adopción e implementación MSPI al interior del IIAP, y para ello identificar el estado de la seguridad de la información, procesos y activos de información críticos, políticas internas, entre otras. Para esto es de suma importancia el compromiso de la Dirección General y las Subdirecciones, que son los tomadores de decisión a nivel institucional.

Al no tener implementado el Modelo de Seguridad y Privacidad de la Información tampoco se cuenta con una herramienta que determine el estado actual de seguridad o inseguridad y esto puede estar generando vulnerabilidades, la norma ISO 27001 define las amenazas como "situaciones que desencadenan en un incidente en la empresa, realizando un daño material o pérdidas inmateriales de sus activos de información". Por otro lado, las vulnerabilidades son definidas en dos sentidos: "uno como la debilidad de un activo que puede ser explotada por una amenaza para materializar una agresión sobre el activo o dos como la potencialidad o la posibilidad de que se materialice una amenaza sobre dicho activo" (*ISO 27001: Vulnerabilidades de La Organización*, n.d.).

No es secreto que la información de cualquier entidad o empresa es uno de sus activos más valiosos, así que no contar con las medidas necesarias para protegerlas, puede causar un gran impacto al momento de un ataque informático o un ciberataque.

Según Mieres (2009), un ataque informático se puede definir como "la manera como se puede aprovechar alguna debilidad o falla (vulnerabilidad) bien sea en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; con la

finalidad de obtener un beneficio". Es importante mitigar los impactos que puedan causar un ataque informático, ya que estos pueden ser muy perjudiciales para una organización.

De acuerdo con el estudio realizado por la Cámara Colombiana de Informática y Telecomunicaciones, en el año 2021 se presentaron 41 billones de intentos de ataques cibernéticos en el mundo y siete billones en Colombia, donde de acuerdo con el último informe de presentado por la Fiscalía General de la Nación, en el año 2021 en Colombia los ataques cibernéticos tuvieron un aumento del 30% respecto del año inmediatamente anterior (Milena et al., 2022), en este documento en su informe respecto del primer trimestre del 2022 arroja importantes respecto de ataques realizados a entidades del Gobierno, en la figura 2 extraída de la citación se puede observar ranking de sitios gubernamentales con mayor exposición de credenciales de usuarios comprometidas.

Figura 2

Ranking de Sitios de dominio gubernamental con mayor exposición de credenciales de usuarios comprometidas

No.	Dominio.gov.co comprometido	Credenciales expuestas	No.	Dominio.gov.co comprometido	Credenciales expuestas
66	muisca.dian.gov.co	3,318	703	www.colpensiones.gov.co:8070	359
226	simo.cnsc.gov.co	1,122	744	jovenesenaccion.dps.gov.co	339
277	www2.icfesinteractivo.gov.co	933	813	www.positivaenlinea.gov.co	307
328	personas.serviciodeempleo.gov.co	766	837	web.sispro.gov.co	296
446	www.icetex.gov.co	555	893	visibles.migracioncolombia.gov.co	273
461	evaluarparaavanzar311.icfes.gov.co	539	910	www.fna.gov.co:8081	265
500	sede.colpensiones.gov.co	499	937	snrbotondepago.gov.co	254
512	oficinavirtual.shd.gov.co	489	943	webazure.dian.gov.co	252
573	community.secop.gov.co	434	1077	solicitudes.icetex.gov.co	213
605	servidorpublico.sigep.gov.co	414	1200	www.medellin.gov.co	192
629	miseguridadsocial.gov.co	404	1244	ecenso.dane.gov.co	182
682	epagos.registraduria.gov.co	373	1297	www.funcionpublica.gov.co	176

Fuente: Cámara Colombiana de Informática y Telecomunicaciones

En el informe anteriormente citado se indica que, en el primer trimestre del 2022, hubo una reducción de aproximada mente el 23% respecto del primer trimestre del 2021, donde para el periodo indicado del 2022 fueron 9.226 denuncias de ciberdelitos frente a 12.012 en el 2021.

En el análisis del phishing y la ley de delitos informático en Colombia (Medina Martínez et al., 2021) plantean que La tecnología de la información continua y evoluciona. Una situación así supone cambios drásticos en la sociedad y en su uso. En cuanto a los usos, como todas las herramientas, pueden tener tanto beneficios como efectos negativos, o usos que se benefician de una minoría pero que tienen un impacto drástico y grande. En respuesta, los gobiernos utilizan sus poderes legislativo, ejecutivo y judicial para establecer leyes y grupos para controlar y procesar a quienes las utilizan con fines delictivos.

Todos los datos anteriores indican la necesidad de proteger eficazmente la información con la que cuenta el IIAP, ya que es una entidad aislada o exceptuada de poder sufrir ataques a su infraestructura tecnológica de cualquier tipo.

1.1 Descripción del área problemática

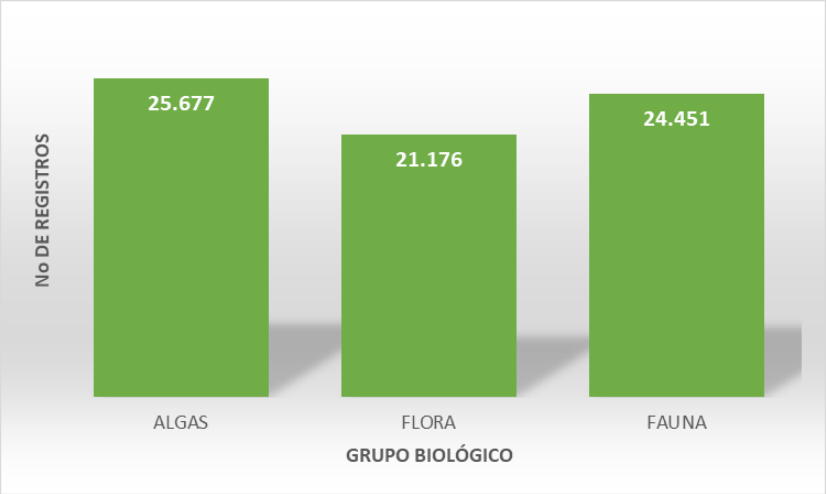
Dentro del Instituto, se enfatiza la importancia del proceso de gestión de la información y el conocimiento. Este proceso juega un papel crucial al ser el medio a través del cual se divulgan los resultados de diversas investigaciones, proyectos y trabajos realizados por la entidad.

Actualmente, el instituto coordina el Sistema de Información Ambiental Territorial del Pacífico Colombiano SIAT–PC, el conjunto integrado de actores, políticas, procesos y tecnologías involucradas en la gestión de información ambiental para facilitar la generación de conocimiento, toma de decisiones, educación y participación social, en el pacífico colombiano (SIAT–PC, 2023), donde realiza resultados de sus investigaciones y trabaja de igual manera con otras entidades del Sistema Nacional Ambiental SINA.

Dentro de los reportes que se realizan están los conjuntos de datos sobre biodiversidad utilizando la herramienta de publicación IPT (Herramienta de Publicación (IPT) de GBIF, 2023) que es una aplicación web de código abierto, disponible de forma gratuita, que facilita la publicación de datos sobre biodiversidad, en esta red el IIAP cuenta con 276 conjuntos de datos publicados en la actualidad, los cuales sobrepasan 70.000 registros de especies entre listas de chequeos y registros biológicos, la figura 3 se pueden ver cómo están repartidos por grupos biológicos:

Figura 3

Registros biológicos según su grupo



Fuente: elaboración propia

Tabla 3 Número de capas geográficas del IIAP

TEMÁTICA / DATASET	NOMBRE DATASET	DESCRIPCIÓN CAPA	FUENTE	AÑO	ESCALA	GEOMETRÍA/ TIPO DATO	GeoDatabase	SIAT-PC
GEOMORFOLOGÍA	t_12_geomorfologia	Unidades Geomorfológicas	IGAC	2015	100k	Polígono	1	1
GEOLOGÍA	t_11_geologia	Fallas Geológicas	SGC	2015	100k	Línea	3	1
		Unidades cronoestratigráfica de geología	SGC	2015	100k	Polígono	3	1
		Pliegue	SGC	2015	100k	Línea	3	1
		Terrenos geológicos	SGC	2015	100k	Polígono	1	1
SUELO	t_14_suelos	Capacidad de Uso de las Tierras	IGAC	2017	100k	Polígono	3	2
		Conflictos de Uso del Territorio	IGAC	2017	100k	Polígono	3	2
		Clasificación de las Tierras por su Oferta Ambiental	IGAC	2017	100k	Polígono	3	2
		Suelos	IGAC	2017	100k	Polígono	3	2
		Clasificación de las Tierras por su Vocación de Uso	IGAC	2017	100k	Polígono	3	2
		Aptitud Forestal	UPRA	2014	100k	Polígono	3	2

TEMÁTICA / DATASET	NOMBRE DATASET	DESCRIPCIÓN CAPA	FUENTE	AÑO	ESCALA	GEOMETRÍA/ TIPO DATO	GeoDatabase	SIAT-PC
		Frontera agrícola	UPRA	2019	100k	Polígono	3	2
HIDROLOGÍA	t_15_hidrologia	Subzonas Hidrográficas	IGAC	2013	100k	Polígono	3	2
		Planes de ordenación y manejo de cuencas hidrográficas - POMCAS	MADS	2021	100K	Polígono	3	
		Humedales	MADS	2021	100k	Polígono	3	2
		Humedales	HUMBOLT	2015	100k	Polígono	1	2
		Zonas Susceptibles de inundación	IDEAM	2016	500K	Polígono	1	2
		Manglar	INVEMAR	2018	100K	Polígono	1	2
		Humedales sitios RAMSAR	MADS	2018	100K	Polígono	3	2
CLIMA	t_19_clima	Clasificación Clima de Caldas Lang 2012	IDEAM	2014	100K	Polígono	1	2
		Clasificación Clima de Lang del 2014	IDEAM	2014	100K	Polígono	1	2
		Clasificación Clima de Lang del 2014	IDEAM	2017	100K	Polígono	1	2

TEMÁTICA / DATASET	NOMBRE DATASET	DESCRIPCIÓN CAPA	FUENTE	AÑO	ESCALA	GEOMETRÍA/ TIPO DATO	GeoDatabase	SIAT-PC
BIOTI_CONTI_COSTE	t_20_biotico_conti_coste	Estaciones Climáticas	IDEAM	2017	100K	Polígono	1	2
		Precipitación anual del 2017	IDEAM	2017	100K	Polígono	1	2
		Radiación Solar Promedio Multianual	IDEAM	2017	100K	Polígono	1	2
		Bosque No Bosque 2018	IDEAM	2018	100k	Polígono	1	2
		Bosque No Bosque 2017	IDEAM	2017	100k	Polígono	1	2
		Bosque No Bosque 2016	IDEAM	2016	100k	Polígono	1	2
		Bosque No Bosque 2015	IDEAM	2015	100k	Polígono	1	2
		Bosque No Bosque 2014	IDEAM	2014	100k	Polígono	1	2
		Bosques Seco Tropical	HUMBOLT	2015	100k	Polígono	1	2
		Ecosistemas continentales, costeros y marinos	IDEAM	2017	100k	Polígono	1	2
		Paramos	MADS	2012	100k	Polígono	1	2
		Coberturas de la tierra 2005 - 2009	IDEAM	2005 - 2009	100k	Polígono	1	2
		Cobertura de la tierra 2010-2012	IDEAM	2010 - 2012	100k	Polígono	1	2

TEMÁTICA / DATASET	NOMBRE DATASET	DESCRIPCIÓN CAPA	FUENTE	AÑO	ESCALA	GEOMETRÍA/ TIPO DATO	GeoDatabase	SIAT-PC
		Cobertura de la tierra 2018	IDEAM	2018	100k	Polígono	1	1
POLITICO_ADMINISTRATIVO	t_22_politico_administrativo	Centros Poblados	DANE	2020	25K	Polígono	1	2
		Centros Poblados	DANE	2020	25k	Polígono	1	0
		Manzanas Sección urbana	DANE	2020	25k	Polígono	1	0
		Sector urbano	DANE	2020	25k	Polígono	1	0
		División veredal	IGAC	2020	100K	Polígono	1	2
SOCIOCULTURAL	t_24_sociocultural	Equipamientos	DANE	2018	25K	Polígono	1	2
AREAS_CONSER_PROTEC_AMBIENTAL	t_31_areas_conser_protec_ambiental	Áreas de conservación y protección en el RUNAP	SPNN	2020	100K	Polígono	1	2
		Paramos	MADS	2012	100K	Polígono	1	2
		Reserva Forestal de Ley Segunda	MADS	2012	100k	Polígono	1	2
AREAS_REGLAMENTACION_ESPECIAL	t_32_areas_reglamentacion_especial	Áreas con Titulación Colectiva a Resguardos Indígenas	IGAC	2021	100K	Polígono	3	2
		Áreas con Titulación Colectiva a Comunidades Negras	IGAC	2021	100K	Polígono	3	2

TEMÁTICA / DATASET	NOMBRE DATASET	DESCRIPCIÓN CAPA	FUENTE	AÑO	ESCALA	GEOMETRÍA/ TIPO DATO	GeoDatabase	SIAT-PC
ZONIFICACION	t_29_zonificacion	Zonificación Reserva Forestal del Pacífico	IIAP	2012	100K	Polígono	1	2
MINERÍA	t_37_mineria	Solicitudes contrato de Concesión 2014	MINMINAS	2014	100K	Polígono	1	2
		Solicitudes contrato de Concesión 2015	MINMINAS	2015	100K	Polígono	1	2
		Solicitudes Legalización ley 1382 2014	MINMINAS	2014	100K	Polígono	1	2
		Solicitudes Legalización ley 1382 2015	MINMINAS	2015	100K	Polígono	1	2
		Solicitudes Legalización ley 685 2014	MINMINAS	2014	100K	Polígono	1	2
		Solicitudes Legalización ley 685 2015	MINMINAS	2015	100K	Polígono	1	2
		Títulos Mineros Otorgados 2014	MINMINAS	2014	100K	Polígono	1	2
		Títulos Mineros Otorgados 2015	MINMINAS	2015	100K	Polígono	1	2
		Zona Minera Comunidades Negras 2014	MINMINAS	2014	100K	Polígono	1	2

TEMÁTICA / DATASET	NOMBRE DATASET	DESCRIPCIÓN CAPA	FUENTE	AÑO	ESCALA	GEOMETRÍA/ TIPO DATO	GeoDatabase	SIAT-PC
		Zona Minera Comunidades Negras 2015	MINMINAS	2015	100K	Polígono	1	2
		Zona Minera de comunidades Indígenas 2015	MINMINAS	2015	100K	Polígono	1	2
TOTAL DE CAPAS GEOGRÁFICAS							**91**	**104**

Fuente: Equipo de laboratorio de datos del IIAP

En la tabla 3 se evidencian las capas geográficas con las que cuenta la entidad, parte de la información georreferenciada y visibiliza a través del SIAT–PC, mediante visor geográfico, son unas 205 capas de diferentes características, sumado las dos bases de datos y distribuidas en diferentes temáticas.

Aunque el proceso de gestión de la información y el conocimiento es importante para la entidad, también resultan significantes los procesos de apoyo y el cumplimiento de normas legales estipuladas para empresas del sector público y privado, entre ellas, las evaluaciones que desde entes de control realizan, como el Índice de Transparencia y Acceso a la Información (ITA), que esta normada por la Procuraduría General de la Nación a través de la ley 1712 de 2014, para este caso el IIPA en su última medición del año 2022 obtuvo una calificación del 76% en el nivel de cumplimiento.

Tabla 4 Resumen medición ITA en el IIAP 2022

Reporte de Cumplimiento ITA para el Periodo 2022		
Categoría de información		
Menú – Nivel I	**Subnivel Menú Nivel II**	**Puntaje Nivel I**
1. Anexo técnico 1. accesibilidad web	1.1. Directrices de Accesibilidad Web	77,8
2. Requisitos sobre identidad visual y articulación con portal único del estado colombiano gov.co	2.1. Top Bar (GOV.CO) 2.2. Footer o pie de página 2.3. Requisitos mínimos de políticas y cumplimiento legal 2.4. Requisitos mínimos en menú destacado	77,3
3. Información de la entidad	3.1. Misión, visión, funciones y deberes 3.2. Estructura orgánica – organigrama 3.3. Mapas y cartas descriptivas de los procesos 3.4. Directorio Institucional incluyendo sedes, oficinas, sucursales, o regionales, y dependencias 3.5. Directorio de servidores públicos, empleados o contratistas 3.6. Directorio de entidades 3.7. Directorio de agremiaciones, asociaciones y otros grupos de interés	73,5

Reporte de Cumplimiento ITA para el Periodo 2022		
Categoría de información		
Menú – Nivel I	**Subnivel Menú Nivel II**	**Puntaje Nivel I**
	3.8. Servicio al público, normas, formularios y protocolos de atención	
	3.9. Procedimientos que se siguen para tomar decisiones en las diferentes áreas	
	3.10. Mecanismo de presentación directa de solicitudes, quejas y reclamos a disposición del público en relación con acciones u omisiones del sujeto obligado	
	3.11. Calendario de actividades	
	3.12. Información sobre decisiones que pueden afectar al público	
	3.13. Entes y autoridades que lo vigilan	
	3.14. Publicación de hojas de vida	
4. Normativa	4.1. Normativa de la entidad o autoridad	80
	4.2. Búsqueda de normas	
	4.3. Proyectos de normas para comentarios	
5. Contratación	5.1. Plan Anual de Adquisiciones	100
	5.2. Publicación de la información contractual	
	5.3. Publicación de la ejecución de los contratos	
	5.4. Manual de contratación, adquisición y/o compras	
	5.5. Formatos o modelos de contratos o pliegos tipo	
6. Planeación	6.1. Presupuesto general de ingresos, gastos e inversión	96,4
	6.2. Ejecución presupuestal	
	6.3. Plan de Acción	
	6.4. Proyectos de Inversión	
	6.5. Informes de empalme	
	6.6. Información pública y/o relevante	
	6.7. Informes de gestión, evaluación y auditoría	
	6.8. Informes de la Oficina de Control Interno	
	6.9. Informe sobre Defensa Pública y Prevención del Daño Antijurídico	
	6.10. Informes trimestrales sobre acceso a información, quejas y reclamos	
7. Trámites	7.1. Trámites	100
8. Participa	8.1. Descripción General	72,7
	8.2. Estructura y Secciones del menú "PARTICIPA"	
9. Datos abiertos	9.1. Instrumentos de gestión de la información	47
	9.2. Sección de Datos Abiertos	
10. Información específica para grupos de interés	10.1. Información para Grupos Específicos.	0

Reporte de Cumplimiento ITA para el Periodo 2022		
Categoría de información		
Menú – Nivel I	**Subnivel Menú Nivel II**	**Puntaje Nivel I**
11. Obligación de reporte de información específica por parte de la entidad	11.1. Normatividad Especial	0
12. Información tributaria en entidades territoriales locales	12.1. Procesos de recaudo de rentas locales	100
	12.2. Tarifas de liquidación del Impuesto de Industria y Comercio (ICA)	
13. Menú atención y servicios a la ciudadanía	13.1. Trámites, Otros Procedimientos Administrativos y consultas de acceso a información pública	100
	13.2. Canales de atención y pida una cita	
	13.3. PQRSD	
14. Sección de noticias	14.1. Sección de Noticias	100
15. Anexo 3. Condiciones técnicas mínimas y de seguridad digital web	15.1. Anexo 3. Condiciones de seguridad digital	100

Al considerar que el IIAP maneja una considerable información desde su misión y sus procesos de apoyo, hace necesario tener una identificación y clasificación de sus activos de información, ya que serían un insumo esencial para generar un análisis riesgos y controles necesarios que minimicen los posibles ataques respecto de la disponibilidad, integridad y confidencialidad de la información que maneja.

1.2 Formulación del problema

Como se ha menciona el Instituto cuenta con un Sistema de Gestión de la Calidad – SGC, en el cual se ha realizado una identificación y valoración de riesgos, cabe aclarar que la metodología utilizada está basada en el estándar ISO 9001:2015, en la tabla número 5, se presenta un resumen de los riesgos identificados en los procesos tanto misionales como de apoyo, resaltando la cantidad de riesgos por cada uno de los procesos, la clasificación según la norma y la cantidad de acuerdo a su clasificación, tal y como se muestra a continuación:

Tabla 5 Matriz de riesgo del SGC en el IIAP.

PROCESO	CANTIDAD DE RIESGOS IDENTIFICADOS	CLASIFICACIÓN DE LOS RIESGOS	CANTIDAD SEGÚN CLASIFICACIÓN DE LOS RIESGOS	TIPO DE PROCESO
Administrativo y financiero	37	Riesgo de tecnología	3	Apoyo
		Riesgos de cumplimiento	20	
		Riesgos financieros	6	
		Riesgos operativos	8	
Control interno	5	Riesgos de cumplimiento	2	Apoyo
		Riesgo estratégico	2	
		Riesgos operativos	1	
Gestión de la información y el conocimiento	14	Riesgo de tecnología	2	Misional
		Riesgo estratégico	4	
		Riesgos de Cumplimiento	3	
		Riesgos operativos	5	
Investigación	13	Riesgo de tecnología	1	Misional
		Riesgo estratégico	1	
		Riesgos de cumplimiento	1	
		riesgos financieros	1	
Jurídico	6	Riesgos operativos	9	Apoyo
		riesgos de cumplimiento	5	
		Riesgos operativos	1	
Planeación	8	Riesgo estratégico	1	Misional
		Riesgos de cumplimiento	4	
		Riesgos operativos	3	
Sistemas de gestión	6	riesgos de cumplimiento	1	Apoyo
		Riesgos operativos	5	
Talento humano	6	Riesgos financieros	1	Apoyo
		Riesgos operativos	5	
TIC	5	Riesgo estratégico	2	Apoyo
		Riesgos operativos	3	
TOTAL	**100**			

Fuente matriz de riesgos SGC IIAP, elaboración propia

Se puede evidenciar un total de riesgos identificados, sobre saliendo los procesos de administrativos y financieros con 37, investigación con 14 y gestión de la información con 13. Aunque estos riesgos no se pueden asociar directamente a un tema de seguridad de la información, son datos que pueden servir para identificar los procesos posibles de interés para identificar los activos de información.

Por otro lado, el proceso TIC es quien menos aporta en riesgos identificados, reiterando que la metodología está basada en la ISO 9001:2015.

En el IIAP hay procesos y procedimientos, pero no se tiene un sistema de seguridad y gestión de la información que establezca controles sobre los atributos de la información (integridad, confidencialidad y disponibilidad).

Por otro lado, sino se toman medidas preventivas adecuadas, los delincuentes cibernéticos pueden atentar contra la información generada o custodiada por la entidad para obtener beneficios o lograr saboteos.

Al no contar el Instituto de Investigaciones Ambientales del Pacífico con un sistema de gestión de la seguridad planeado e implementado surge el siguiente interrogante:

¿Cómo controlar los riesgos y asegurar que la información de los procesos misionales y de apoyo en el Instituto de Investigaciones Ambientales del Pacífico conserve su Integridad, Confidencialidad y Disponibilidad?

1.3 Justificación

Las entidades de la rama ejecutiva del orden nacional, para este caso el Instituto de Investigaciones Ambientales del Pacífico, deben cumplir con lo dispuesto en la ley 1341 de 2009 y reglamentada mediante los decretos 2573 de 2014 y 1078 de 2015, en las cuales se expone que es de vital importancia promover condiciones de ciberseguridad en la información que posee en

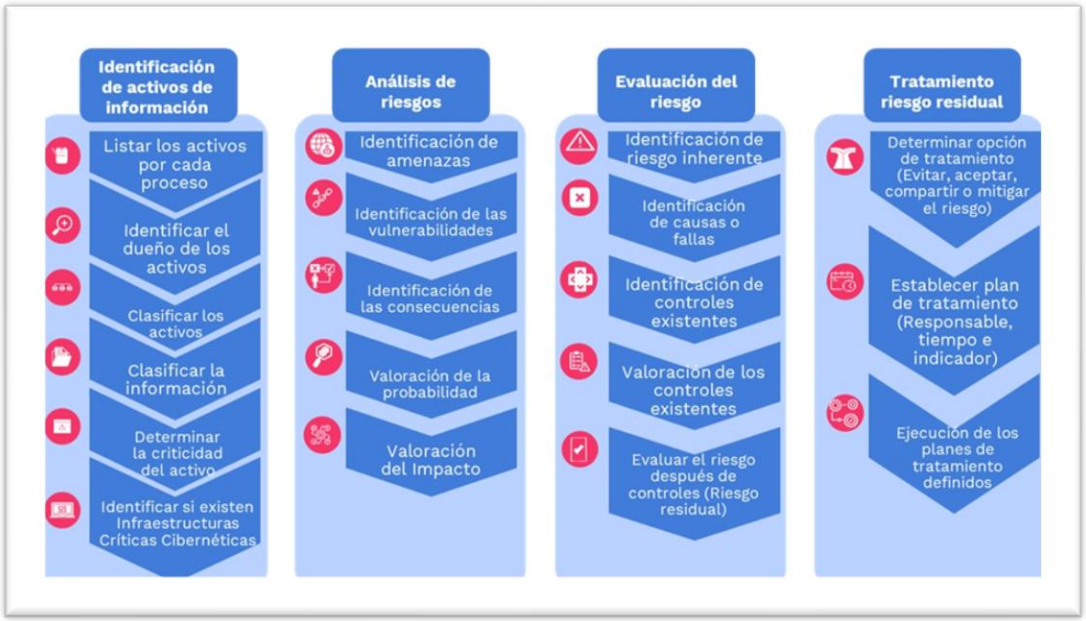
sus dispositivos o circulan por la red, por lo cual esta actividad transversal es obligatoria y con la ejecución del presente trabajo se inicia la alineación de las políticas de programa de Gobierno Digital, que le permitirá cerrar la brecha que existe en la actualidad aproximándose a un eficiente Sistema de Gestión de Seguridad Institucional.

También, cualquier empresa pública y privada debe conocer la seguridad y privacidad de los datos y equipos que administra y que para estas entidades tienen requerimientos legales especiales para el manejo de información de sus usuarios, por lo que podrían estar inmersos en procesos legales por su inobservancia.

Para el año 2021 El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) expide la Resolución 500 de 2021, "por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital" (MinTIC, 2021). En la figura 4 se observa el modelo de seguridad y privacidad de la información según los lineamientos dictados.

Figura 4

Modelo Seguridad y Privacidad de la Información - MSPI



Fuente: Modelo de seguridad y privacidad de la información, (MinTIC, 2021).

Para el caso apoyado en el MSPI, hay que hacer un diagnóstico del estado actual de la seguridad de la información, pudiendo identificar sus activos de información y su clasificación, para poder hacer una valoración y análisis de riesgos para determinar controles que mitigue la posible ocurrencia de uso o acceso indebido a la información generada o custodiada en el IIAP.

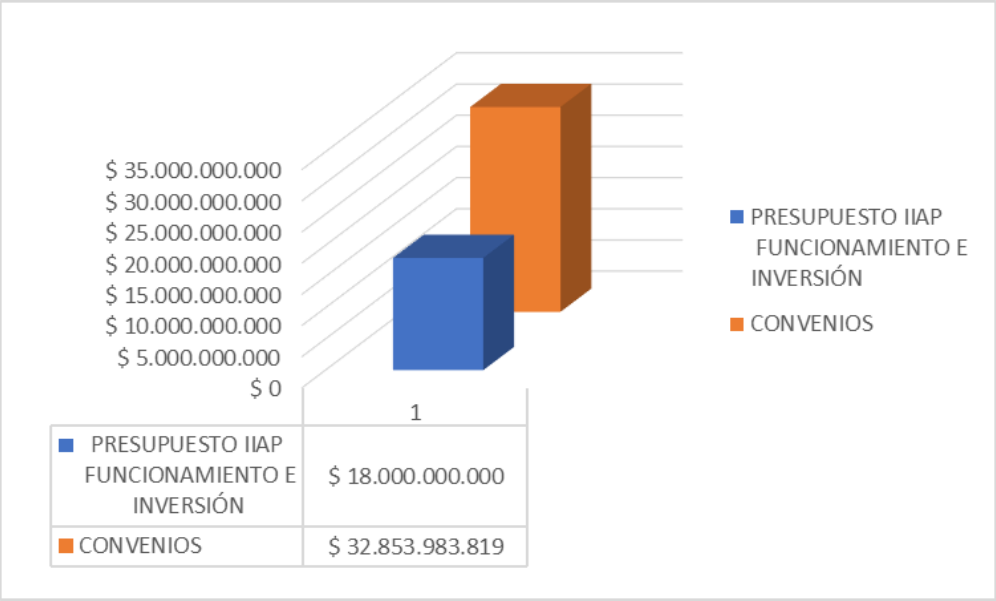
Todas estas actividades deben servir para una política institucional de seguridad de la información, que protege los activos de información vital de los procesos y procedimientos misionales y del apoyo en el Instituto de Investigaciones Ambientales del Pacífico.

En el año 2023, tras la gestión desde la Dirección General del IIAP, se logró firmar convenios con montos adicionales superiores a los $32.000.000 de pesos, 183% frente al presupuesto anual de la entidad, pero esto demuestra la confianza de la entidad respecto al

trabajo que realiza, es un reto más para tener medidas que garantice la salvaguarda correctamente, cumpliendo con los estándares de seguridad de la información.

Figura 5

Comparativa de presupuestos oficial 2023 Vs convenios 2023



Fuente: presupuesto oficial IIAP 2023, elaboración propia.

Teniendo presente el crecimiento en convenios y proyectos en ejecución, así como los montos financieros para la entidad, no contar con medidas y políticas clara en lo relacionado con la seguridad de la información y sobre todo respecto de sus activos de información es un alto riesgo, que puede conllevar a afectaciones legales, económicas y disciplinarias de impactos incalculables en el IIAP, lo que hace de este trabajo de investigación una herramienta que debe servir para la formulación y gestión de sus respectivos planes estratégicos.

2. Objetivos

2.1. Objetivo general

Diseñar el sistema de gestión de seguridad de la información con base en el Modelo de Seguridad y Privacidad de la Información – MSPI y la familia de normas ISO 27000:2022 en el Instituto de Investigaciones Ambientales del Pacífico – IIAP.

2.2. Objetivos específicos

- Establecer la línea base de seguridad de la información y así determinar el alcance a lograr en el Sistema de Gestión de seguridad de la información en el IIAP.
- Construir la política del Sistema de Gestión de Seguridad de la Información.
- Identificar y clasificar los activos de información, realizar el análisis de impactos y el análisis de riesgos con base en lo dispuesto por MinTIC en el MSPI y el estándar de la ISO 27005.
- Determinar los controles óptimos, según las amenazas y vulnerabilidades evidenciadas, con base en el estándar ISO 27002:2022 y la guía de controles de seguridad y privacidad de la información, logrando la declaración de aplicabilidad.

3. Antecedentes

Los proyectos precedentes, sobre los SGSI, permiten ampliar el espectro de la estructura, formulación y desarrollo de este trabajo, que ayudan a desarrollar objetivos y planificar el sistema de gestión de seguridad de la información basado en el MSPI.

El Ministerio de la Comunicación ha propuesto un Modelo de Seguridad y Privacidad de la Información – MSPI, el cual plantea una ejecución encaminada a que las entidades identifiquen el nivel de madurez que han desarrollado en cuanto a seguridad de la información y a partir de esta identificación, iniciar un ciclo PHVA sostenible (MinTIC, 2011), que resulta ser la guía referente para este trabajo.

Aunque las iniciativas del Gobierno han buscado que las entidades públicas pongan a disposición de la ciudadanía, información y datos generados o custodiados por estas, nacen tensiones naturales, respecto de la protección y la pérdida de privacidad. En su artículo que expone la seguridad y la privacidad como convergentes, Cano (2012) indica que, es importante tener políticas y lineamientos muy claros que conlleven a confiar en el buen uso y manejo de la información, sensible para las organizaciones y las personas comunes. Al ir indagando y consultando literatura y hablar de seguridad de la información aparecen preguntas asociadas a nuevos temas como son los riesgos y la gestión de los mismos, esta evolución involucra temas claves como Cyber Riesgos y Seguridad de la Información, aquí cobra importante relevancia la gestión de seguridad sobre terceros involucrados en los procesos de negocio, incluyendo la protección de datos personales, capitulo en el cual las empresas y entidades en Latino América, tienen un largo camino por recorrer (DELOITTE, 2016).

Tristancho, (2015) en su trabajo se pregunta ¿Por qué se fracasa en las implementaciones de los SGSI? Resaltando que, aunque las TI resultan herramientas importantes en la seguridad de

la información, se requiere que se incorporen como parte integral de la planificación y no un instrumento aislado de los objetivos de la empresa o entidad. Igualmente en 2015 al diseñar un SGSI en una entidad financiera de segundo piso, con referencia a la ISO/IEC 27001:2013, se estableció que la integralidad de un sistema de seguridad en una organización va más allá de una herramienta TI para mitigar los riesgos, que se deben considerar aspectos importantes como el cumplimiento de la norma, controles orientados a proteger la información intercambiada con terceros, establecer procesos de gestión de incidentes de seguridad, políticas de seguridad aprobadas por la Alta Dirección, elaborar planes de capacitación, formación y sensibilización en seguridad (Guzmán, 2015).

Dentro de las búsquedas específicas, son pocos los trabajos o investigaciones que traten sobre el MSPI, y que estén desarrollados en entidades Sistema Nacional Ambiental - SINA, pero si es importante hablar de gobierno y gestión de TI en las entidades públicas, dejando claro la diferencias y relaciones entre gobierno y gestión TI y los roles que juegan los actores de las entidades públicas, esto para garantizar una adecuada articulación con la sociedad en general, (López et al., 2017), por su parte Aguilar et al. (2017) señala que la gestión de TI es clave para triunfar en los gobiernos de TI que no se gestiona adecuadamente como un ítem estratégico para cumplir las metas y objetivos principales de muchas entidades, dejando claro la falta de marcos o guías metodológicas para ayudar a los altos ejecutivos y profesionales de TI en la organización a administrar la demanda de TI.

Pese a la poca información en entidades SINA, el trabajo realizado en la Corporación Autónoma Regional de Cundinamarca–CAR, en 2017, que diagnóstico y planifico el SGSI en esta entidad, identificando como uno de los inconvenientes la falta de compromiso de la Dirección respecto a la implementación de un MSPI, que además encuentra obstáculo para

identificarse bien sus activos de información y generar políticas y controles que permitan salvaguardar de una mejor manera estos, (Villamil Ávila, 2017), ahora por el área de influencia del IIAP y su sede principal, Chocó.

Contar con una metodología que permita de una manera organizada el diseño en implementación de un SGSI, teniendo especial énfasis en la seguridad de la información, los controles de seguridad, la guía para la implementación de un SGSI y la gestión del riesgo, todo esto basado en la familia de la de normas de la ISO/IEC 27000 (Valencia & Orozco, 2017), por su parte Silva & Jara (2017) destacan en el trabajo realizado en el fondo pasivo social Ferrocarriles Nacionales de Colombia, que Diseño un MSPI que tomo el cumplimiento de la estrategia gobierno en línea como soporte y estableció que si bien es importante tener una metodología, conocer el estado de madurez o de implementación, es de igual relevancia al momento del diseño del modelo de seguridad y privacidad, así como concebir la seguridad de la información como un tema clave para el logro de sus objetivos empresariales.

Estos artículos o trabajos de grados que se han realizado, siguen dejando claro la importancia de contar con la gobernanza y la gestión de TI, lo que garantiza generar valor y alcanzar mayores índices de competitividad, encontrando cifras relacionadas a criterios como Beneficios (55%), Recursos (24%) y Riesgos (21%), (Vanti et al., 2018), con datos como estos cobra mayor relevancia la necesidad implementar de manera efectivas controles capaces de mitigar en gran proporción la información de las empresas o entidades.

Estudios como el realizado en entidades sector financiero confirman la importancia de planificar muy bien los SGSI, que determina como relevantes tener claramente identificados activos de información, principales riesgos de seguridad de la información, el tratamiento de

dichos riesgos, contar con políticas y lineamientos claros, así como un modelo basado en los dominios de la familia de la norma ISO 27001:2013, (Moscaiza, 2018). En trabajos de grados realizados en entidades públicas específicamente, con literaturas como fuente, se llegan a conclusiones como que las personas son importantes para el éxito o fracaso en la implementación de un SGSI, de ahí la importancia de tener en cuenta distintos factores, como el legal, socio cultural, organizacional, entre otros, (Cardona & Carvajal, 2018). Haga clic o pulse aquí para escribir texto. Conclusiones muy parecidas y compartidas en el estudio realizado en la Alcaldía de Puerto Asís – Putumayo, en sus fases de diagnóstico y planificación respecto del modelo de privacidad de la información, (Sierra & Hurtado, 2018).

Teniendo en cuenta las conclusiones de los estudios anteriores, cobra gran relevancia, cumplir con los requisitos de la norma, sobre todo lo referente a la ISO 27001:2013, que con una mira holística cumple con los requisitos, para gestionar riesgos a través de controles eficientes, (Stoll, 2018).

Ante los inconvenientes de la literatura analizada, se inicia a observar la necesidad de modelos que coadyuven a implementar un sistema de gestión de seguridad de la información, como un modelo de gobernanza TI, es donde el MSPI cobra importancia porque integra prácticas que alinean objetivos de gobierno y gestión del modelo de seguridad y privacidad de la información (Rojas et al., 2019). Haga clic o pulse aquí para escribir texto. Para cumplir estos objetivos de un MSPI, el gobierno de datos es muy importante, ya que los datos terminan siendo valiosos y por ende se debe propiciar por proteger de la mejor manera posible, (Abraham et al., 2019).

Teniendo presente que las postura respecto de SGSI y sus implicaciones tiene una importancia según el sector o la empresa en la cual se piense implementar, (Hamdi et al., 2019),

en la realización de búsqueda de literatura sobre seguridad de la información, cobra relevancia un tema como la ciberseguridad, la cual no se aleja de los principios de los estándares respecto de gestión de riesgos y controles que se deben tener en cuenta, máxime para temas concernientes con Normativa gubernamental en ciberseguridad: Marco, estándares y recomendaciones, (Srinivas et al., 2019).

Entre los artículos consultados, destaca la integración entre la ISO/IEC 27001:2013 y el MSPI, donde se puede corregir las directrices, dominios y controles inmersas en la norma y que el modelo adopta en un cien por ciento (Benavides, 2019), el uso de TI busca crear una ventaja competitiva en los negocios. Sin embargo, existen muchas organizaciones que no tienen un control adecuado de estas tecnologías y no les permiten alcanzar los objetivos deseados, por esta razón es importante administrar y controlar adecuadamente las TI a través de un marco de gobierno de TI, (Aguilar & Vergara, 2020).

Como antecedente se resalta las conclusiones obtenidas en el estudio del diseño SGSI para la empresa ORIENT., (Navarro, 2020) Lo cual es compartido en el documento Propuesta metodológica para implementar un marco de referencia de gobierno y gestión de las Tecnologías de Información en las entidades del sector de la economía solidaria de primer nivel de supervisión, (González, 2021).

Después de revisar muchas búsquedas, presentar una revisión de la literatura académica sobre ISO/IEC 27001, el estándar más reconocido para la seguridad de la información, se identifican en cinco focos generales de investigación: relación con otros estándares, motivaciones, problemas en la implementación, posibles resultados y factores contextuales, (Culot et al., 2021).

La relación entre el MSPI y la familia ISO 27000 es que el primero se basa en los requisitos y controles del segundo, pero los adapta al contexto colombiano y a las necesidades específicas de las entidades públicas. El MSPI no es una norma certificable, sino una guía de implementación que orienta la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (MinTIC, n.d.).

Por lo tanto, el MSPI y la familia ISO 27000 son complementarios, pero no obligatorios. El MSPI busca aprovechar los beneficios de los estándares internacionales, pero también considerar las particularidades del sector público colombiano. El MSPI es una herramienta que facilita el cumplimiento de la política de Gobierno Digital y la estrategia de seguridad digital en el país.

Por otro lado, se debe tener en cuenta que los estándares y modelos deben ir de la mano con el avance en las legislaciones y los delitos informáticos, con base en esto se realizó un estudio de derecho comparado entre la ley de delitos informáticos vigente en Colombia, y los punibles de tal naturaleza tipificados en las legislaciones nacionales de Perú, Chile, Alemania y España, al hacerlo, los autores cumplieron con las disposiciones del Convenio de Budapest sobre Ciberdelincuencia. Desde un enfoque cualitativo descriptivo, se presentó una descripción del contenido y alcance de los instrumentos jurídicos internacionales mencionados, refiriéndose a la clasificación y composición de actos señalados en la Ley 1273 de 2009, que crea un nuevo bien jurídico tutelar de protección de información y datos, además de la Ley 1928 de 2018, que ratificó el Convenio sobre Delito Cibernético, logrando con este desarrollo, conocer de diferentes maneras cómo se entienden y sancionan actos delictivos virtuales. (Mejía-Lobo et al., 2023).

4. Referente normativo y legal

A continuación, se presenta un contexto general del marco normativo que se debe tener en cuenta en el contexto colombiano y según el tipo de Organización sobre los aspectos de Seguridad de la Información:

NORMA	DESCRIPCIÓN
Constitución Política de Colombia. Artículos 15, 209 y 269.	Artículos que consagran lo relacionado con el derecho a la intimidad personal y familiar, al buen nombre, a conocer, actualizar y rectificar las Informaciones que se hayan recogido sobre las personas en bancos de datos y archivos, y a la inviolabilidad de la correspondencia y demás formas de comunicación privada.
Ley 1581 de 2012.	Por la cual se dictan disposiciones generales para la protección de datos personales alineado con la 27701
Decreto 2609 de 2012.	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Decreto 886 de 2014.	Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Ley 1712 de 2014.	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1074 de 2015.	Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
Decreto 1078 de 2015.	es el decreto único reglamentario del sector de tecnologías de la información y las comunicaciones, expedido por el presidente de la República de Colombia, con el fin de simplificar y racionalizar el ordenamiento jurídico de este sector.
Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública, en el cual se establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de 11. Gobierno Digital, antes Gobierno en Línea y 12. Seguridad Digital.
CONPES 3854 de 2016.	Política Nacional de Seguridad digital, estrategia del gobierno colombiano para crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital
Ley 1915 de 2018.	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

NORMA	DESCRIPCIÓN
Decreto 612 de 2018.	Es una norma que establece las directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. El decreto tiene como objetivo simplificar y racionalizar el ordenamiento jurídico del sector de tecnologías de la información y las comunicaciones, y facilitar el seguimiento y la evaluación de la gestión y el desempeño institucional.
Decreto 2106 de 2019	Establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los Lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
Ley 2052 de 2020.	Por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial y a los particulares que cumplan funciones públicas y/o administrativas, en relación con la racionalización de trámites y se dictan otras disposiciones.
Resolución 500 de 2021, expedida por el MinTIC	Estableció los lineamientos y estándares para la estrategia de seguridad digital, y la adopción del modelo de seguridad y privacidad, como habilitador de la política de Gobierno Digital. En consecuencia, la seguridad y privacidad de la información, y el Modelo de Seguridad y Privacidad de la Información adoptado.
Resolución 460 de 2022, expedida por el MinTIC	Plan Nacional de Infraestructura de Datos estableciendo los lineamientos generales para su implementación, con el fin de impulsar la toma de decisiones basadas en datos de los sujetos obligados a la Política de Gobierno Digital, a partir del aumento, uso y aprovechamiento de la información e incorporando el enfoque de datos como infraestructura.
Resolución 0746 de 2022 (MinTIC)	Esta resolución tiene como objetivo garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de las funciones de las entidades públicas, en un entorno de confianza digital y de gestión de riesgos. La resolución se compone de 14 artículos
Decreto 767 de 2022	Norma que actualiza la política de Gobierno Digital del país, con el fin de impactar positivamente la calidad de vida de los colombianos y de incrementar la competitividad del país. El decreto establece los lineamientos generales de la política, que se basa en los elementos de gobernanza, cultura y apropiación, innovación pública e iniciativas dinamizadoras de transformación digital.

5. Referente teórico

La teoría del trabajo está en la familia de la norma ISO/IEC 27000, emitida por la Organización Internacional de Normalización (ISO) y que trata de cómo gestionar la seguridad de la información en cualquier organización. La base de la ISO/IEC 27001, cuya revisión más reciente se publicó en 2022 y ahora su nombre completo es ISO/IEC 27001:2022. La primera revisión de esta norma se publicó para el año en 2005 y con la norma británica BS 7799-2. Por consiguiente, se expone los principales conceptos relacionados con esta norma.

5.1. Seguridad de la Información:

La seguridad de la información, según la ISO 27001(*SGSI*, n.d.) consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen los pilares sobre los cuales se edifica lo relacionado con la seguridad de la información:

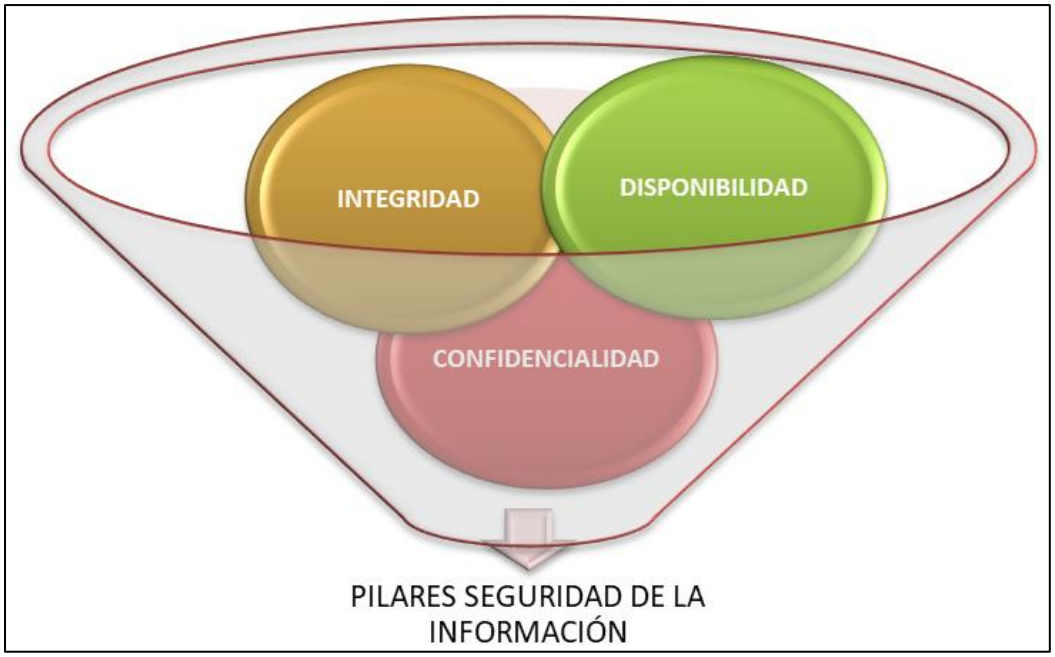
- **Confidencialidad: la garantía del acceso a la información solo por el o los usuarios debidamente autorizados.** Por definición desde la norma es la "propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados" (*Glosario de Términos y Definiciones ISO 27000 - ISO 27001*, n.d.).
- **Disponibilidad:** que definida desde la noma es la "Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada" (*Glosario de Términos y Definiciones ISO 27000 - ISO 27001*, n.d.), que visto desde una organización es esa información que debe ser accesible para todo el personal, tanto interno como externo en el momento que se desee o requiera.

- **Integridad:** La integridad hace referencia todo lo concerniente a la precisión, coherencia y completitud. Desde la norma "La integridad de la información se refiere a la exactitud y consistencia generales de los datos o expresado de otra forma, como la ausencia de alteración cuando se realice cualquier tipo de operación con los datos, lo que significa que los datos permanecen intactos y sin cambios" (*Glosario de Términos y Definiciones ISO 27000 - ISO 27001*, n.d.).

Según Chicano (2015) en su libro Gestión de incidentes de seguridad informática. IFCT0109, para que la seguridad de la información cumpla unos apropiados patrones de seguridad se debe garantizar el cumplimiento de las tres propiedades enunciadas anteriormente de manera correcta.

Figura 6

Propiedades la información



Fuente: Elaboración propia

Gestión de Seguridad de la Información: La seguridad de la información incluye la protección de información, sistemas, recursos y demás activos contra desastres, errores (intencionales o no) y manipulación no autorizada, para reducir la probabilidad y el impacto de los incidentes de seguridad.

Según la norma ISO/IEC 27002:2007, la seguridad de la información es proteger la información contra las amenazas para garantizar la continuidad del negocio, minimizando los riesgos y maximizando el retorno sobre la inversión y las oportunidades de negocio.

La seguridad de la información se obtiene gracias a la implementación de controles, con políticas, procesos, procedimientos, estructuras organizacionales y funciones de hardware y software.

Los controles deben establecerse, implementarse, monitorearse, evaluarse y mejorarse continuamente para cumplir con los objetivos del negocio y la seguridad de la organización. La identificación de los controles adecuados requiere una planificación detallada. A continuación, se especifican algunos conceptos:

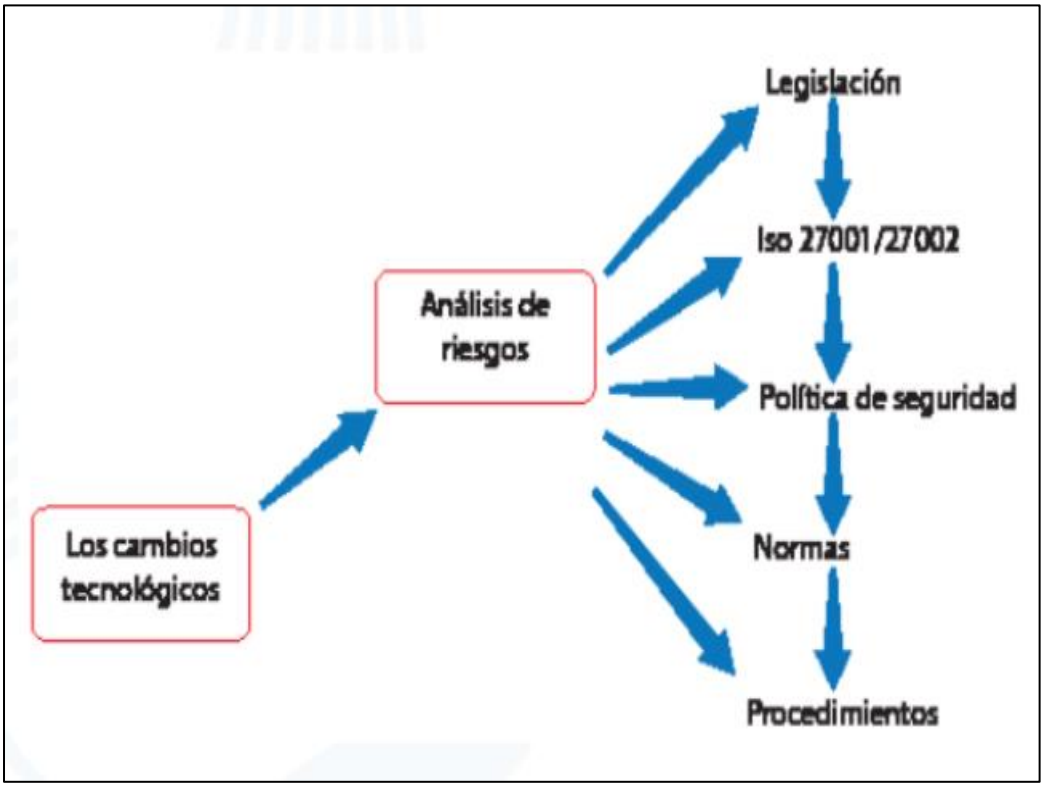
- **Incidente de seguridad:** corresponde a cualquier evento adverso relacionado con la seguridad, por ejemplo, ataques de denegación de servicio (Denial of Service, DoS), robo de información, fuga y la obtención de un acceso no autorizado a la información.
- **Activo:** cualquier elemento que tenga valor para la organización y su negocio. Algunos ejemplos: bases de datos, software, equipos (computadores, notebooks), servidores, dispositivos de red (routers, switches, etc.), personas, procesos y servicios.
- **Amenaza:** cualquier evento que explote vulnerabilidades. Causa potencial de un incidente no deseado, que puede resultar en daños a un sistema u organización

- **Vulnerabilidad:** cualquier debilidad que puede ser explotada y ponga en peligro la seguridad de los sistemas y datos. Fragilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas. Las vulnerabilidades son fallas que permiten la aparición de deficiencias en la seguridad general del equipo o de la red. Configuraciones incorrectas en el equipo o en la seguridad también permiten la creación de vulnerabilidades. A partir de esta falla, las vulnerabilidades son explotadas por amenazas que cuando se materializan, causan daños al computador, a la organización o a los datos personales.
- **Riesgo:** combinación de la probabilidad (oportunidad de que la amenaza se materialice) de que ocurra un evento y sus consecuencias para la organización. Algo que puede ocurrir y sus efectos sobre los objetivos de la organización.
- **Ataque:** cualquier acción que comprometa la seguridad de una organización.
- **Impacto:** resultado evaluado de un evento en particular.

La Figura 7 presenta una visión de la seguridad de la información. Una mirada que encuentra en los cambios tecnológicos un aspecto preponderante el cotidiano hacer de las organizaciones. Esas variaciones tecnológicas pueden llevar a que se presenten nuevas vulnerabilidades y riesgos, o agravar los ya existentes, motivos que se deben tener presente al evaluar los riesgos dinámicas, permitiendo levantar los niveles de riesgo y tratarlos.

Figura 7

Visión general de la seguridad de la información



Sistema de gestión de seguridad de la información (SGSI): Es parte del sistema de gestión global de una organización, basado en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. Este sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

5.2. Norma ISO 27001.

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

La revisión más reciente de esta norma fue publicada en 2022 y ahora su nombre completo es ISO/IEC 27001:2022. La primera revisión se publicó en 2005 y fue desarrollada con base en la norma británica BS 7799-2.

La ISO 27001 puede implementarse en cualquier organización independiente su razón comercial y tamaño. Gracias a que un grupo de especialistas aporta metodologías para diseñar, implementar y mejorar la gestión de la seguridad de la información en las organizaciones que deseen acogerla. Estas empresas logran certificar los procesos que requieren y necesitan sobre la norma ISO 27001 y de esta manera se confirma que la organización la tiene implementada.

¿Cómo funciona la ISO 27001? "El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando los potenciales problemas que podrían afectar la información (la evaluación de riesgos) y luego definiendo qué es necesario hacer para evitar que se produzcan (mitigación o tratamiento del riesgo).

Este estándar también incluye la evaluación de riesgos de seguridad de la información y los requisitos de manejo que satisfacen las necesidades de las empresas, algunos puntos indispensables en la aplicación de la norma para la creación de un SGSI son:

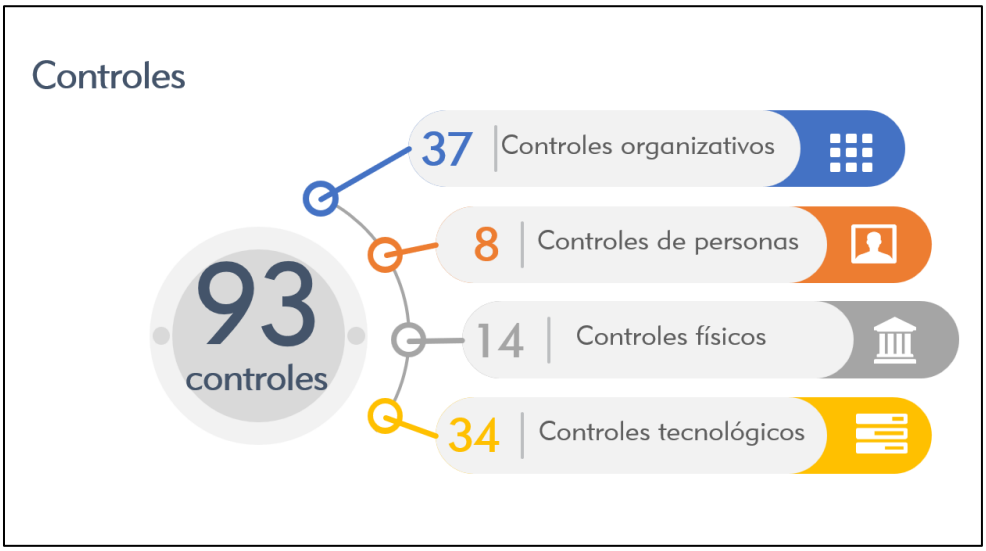
- Definir las políticas de SI.
- Establecer el alcance claro del SGSI
- Realizar la evaluación del análisis de riesgo
- Elegir los controles de seguridad de la información.
- Definir competencias con las que se cuentan dentro de la organización.
- Establecer el mapa de riesgos.

- Definir autoridades y responsabilidades.
- Poner en marcha el Plan de gestión de riesgos establecido.
- Aplicación del SGSI.
- Escoger y establecer los controles de seguridad, que se aplican al manejo de los riesgos.
- Revisar internamente el SGSI.
- Realizar auditorías periódicas y acciones correctivas.
- Revisar los indicadores y métricas del SGSI.

La figura 8 muestra el listado de controles en los cuales se enfoca la norma ISO27001:2022

Figura 8

Resumen del Anexo A - ISO 27001:2022



Fuente: Global trust association

5.3 Norma ISO 27005.

Es un estándar internacional que proporciona orientación para la gestión de riesgos de seguridad de la información, ciberseguridad y protección de la privacidad. Esta norma se alinea

con la ISO/IEC 27001:2022, que especifica los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI). La ISO/IEC 27005:2022 también se basa en la ISO 31000:2018, aplicando a cualquier organización que quiera gestionar los riesgos que puedan comprometer su seguridad de la información. Su versión actualizada se conoce como ISO/IEC 27005:2022.

El objetivo de la ISO 27005:2022 es el de ayudar a las organizaciones a identificar, analizar, evaluar, tratar y monitorear los riesgos de seguridad de la información que pueden afectar a sus activos, procesos, personas y partes interesadas. La norma ofrece dos enfoques para la identificación de riesgos: el enfoque basado en eventos y el enfoque basado en activos. El primero se centra en los eventos que pueden causar daños a la seguridad de la información, mientras que el segundo se centra en los activos que pueden ser afectados por dichos eventos. La norma incluye en el anexo A criterios de riesgo de seguridad de la información, factores utilizados para determinar la importancia de los riesgos y decisiones sobre su tratamiento. Estos criterios incluyen: (a) el nivel de riesgo aceptable, (b) la escala de probabilidad, (c) la escala de consecuencia y (d) la matriz de riesgo. Esta norma es aplicable a todas las organizaciones que deseen implementarla, independientemente de su tipo, tamaño o sector, que quieran gestionar los riesgos de seguridad de la información de forma sistemática y coherente.

La ISO 27005:2022 se estructura en siete cláusulas de la siguiente manera:

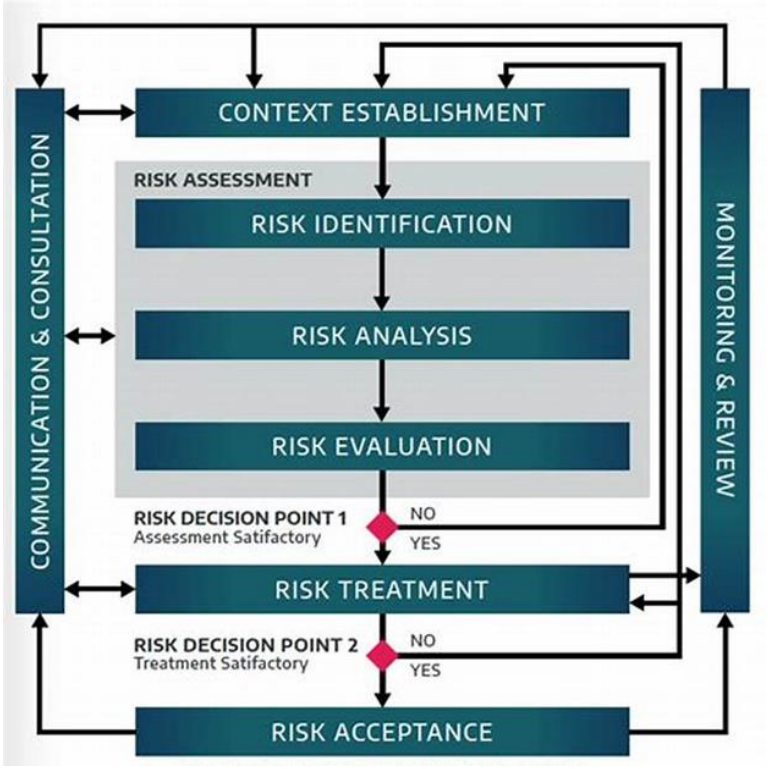
1. Alcance.
2. Términos y definiciones.
3. Principios.
4. Responsabilidades.

5. Gestión de riesgos de seguridad de la información.
6. Técnicas prácticas.
7. Anexo informativo.

- La cláusula 5 describe el proceso de gestión de riesgos de seguridad de la información, que consta de seis etapas: (a) establecimiento del contexto, (b) identificación de riesgos, (c) análisis de riesgos, (d) evaluación de riesgos, (e) tratamiento de riesgos y (f) monitoreo y revisión de riesgos. Tal y como se puede observar en la figura 9:

Figura 9

Estructura de la ISO 27005



5.4. Norma ISO 27032.

La norma ISO 27032:2023 es una norma internacional que proporciona directrices para la ciberseguridad, entendida como la seguridad de la información en el ciberespacio. El ciberespacio es el entorno complejo de la interacción de personas, software y servicios en Internet mediante dispositivos tecnológicos y redes conectadas a él. La norma tiene como propósito ayudar a las organizaciones a mejorar su capacidad de prevenir, detectar, responder y recuperarse de los incidentes de ciberseguridad que puedan afectar a sus activos, procesos, personas y partes interesadas. La norma se alinea con otras normas de la serie ISO 27000, como la ISO 27001, que especifica los requisitos para un sistema de gestión de seguridad de la información, o la ISO 27005, que proporciona directrices para la gestión de riesgos de seguridad de la información. La norma se publicó por primera vez en 2012 y se actualizó en 2023, incorporando cambios significativos como el cambio de nombre del documento, la inclusión de conceptos relacionados con los escenarios de riesgo, la orientación para contrastar los dos enfoques para la identificación de riesgos y la consolidación de los anexos en uno solo (Arévalo, 2022).

La norma incluye conceptos, principios, procesos y técnicas para la gestión de la ciberseguridad, así como orientación sobre el uso de tecnologías, herramientas, políticas, buenas prácticas y estándares para la protección de los activos digitales, las aplicaciones, los servidores, las personas y los usuarios. La norma se puede aplicar a cualquier tipo de organización, independientemente de su tamaño, sector o actividad. Algunos de los aspectos que se destacan en la norma son:

- Evaluación de riesgos cibernéticos: La norma recomienda llevar a cabo evaluaciones periódicas de los riesgos cibernéticos que enfrenta una organización,

utilizando métodos y criterios apropiados. Esto permite identificar vulnerabilidades y establecer estrategias para protegerse contra posibles ciberataques. La norma ofrece dos enfoques para la identificación de riesgos: el enfoque basado en eventos y el enfoque basado en activos. El primero se centra en los eventos que pueden causar daños a la seguridad de la información, mientras que el segundo se centra en los activos que pueden ser afectados por dichos eventos. La norma también incluye un anexo con criterios de riesgo de seguridad de la información y técnicas prácticas para la gestión de riesgos de seguridad de la información (Guzmán-Solano, 2019).

- Colaboración y coordinación: La norma alienta la colaboración y coordinación entre diferentes actores, como gobiernos, empresas, organismos reguladores y la sociedad civil, para mejorar la resistencia frente a amenazas cibernéticas. La norma propone un marco de referencia para la cooperación entre las partes interesadas, basado en el concepto de ciber resiliencia, que implica la capacidad de adaptarse y recuperarse de los incidentes de ciberseguridad. La norma también sugiere mecanismos para compartir información, experiencias y buenas prácticas, así como para establecer roles y responsabilidades claros en la gestión de la ciberseguridad (Moreano et al., 2023).
- Gestión de incidentes: La norma destaca la importancia de tener planes de gestión de incidentes bien definidos para responder eficientemente a ataques cibernéticos. Estos planes incluyen la detección temprana, la contención del incidente, la recuperación rápida y la mejora continua. La norma también proporciona directrices para la comunicación y la notificación de los incidentes, tanto interna

como externamente, así como para la evaluación y el análisis de las causas y las lecciones aprendidas (Guzmán-Solano, 2019).

- Sensibilización y capacitación: La norma sugiere programas de sensibilización y capacitación para asegurar que todos los involucrados en la ciberseguridad comprendan la importancia de mantener una postura segura en el mundo digital. La norma recomienda que se identifiquen las necesidades de formación de los empleados y usuarios, se diseñen e implementen planes de capacitación adecuados, se evalúen los resultados y se realicen acciones correctivas si es necesario. La norma también enfatiza el papel de la cultura organizacional y el liderazgo en la promoción de la ciberseguridad.

La ISO 27032 aborda aspectos clave como la evaluación de riesgos cibernéticos, la colaboración y coordinación entre las partes interesadas, la gestión de incidentes y la sensibilización y capacitación. La norma se puede aplicar a cualquier tipo de organización, independientemente de su tamaño, sector o actividad. La implementación de la norma puede aportar beneficios como la protección de la información y los sistemas informáticos, la mejora de la confianza y la reputación, el cumplimiento de los requisitos legales y regulatorios, la reducción de los costos y las pérdidas asociados a los ciberataques y la mejora de la competitividad y la innovación. Sin embargo, la implementación de la norma también implica desafíos como la necesidad de contar con recursos humanos, técnicos y financieros suficientes, la adaptación a los cambios constantes del entorno digital, la coordinación con múltiples actores y la medición del impacto y la efectividad de las acciones realizadas. Por lo tanto, se recomienda que las organizaciones que quieran adoptar la norma realicen un diagnóstico previo de su situación actual, definan sus objetivos y prioridades, establezcan un plan de acción y un

cronograma, asignen responsabilidades y recursos, monitoreen y evalúen el proceso y realicen mejoras continuas. Asimismo, se recomienda que las organizaciones busquen el apoyo y la asesoría de expertos y entidades certificadoras que puedan orientarlas y acompañarlas en la implementación de la norma.

Norma ISO 31000.

Por la gran importancia de la gestión de riesgos hoy, existen estándares como ISO 31000, que propone procesos y métodos para gestionar y reducir el impacto de los riesgos para las organizaciones. Una organización está continuamente expuesta a diferentes tipos de amenazas, las cuales no solo son externas sino también internas, este tipo de amenaza es una gran preocupación porque puede afectar los objetivos de la empresa, para lo cual la normativa propone una serie de mecanismos con los que busca identificar, analizar, evaluar y mitigar el impacto de un riesgo.

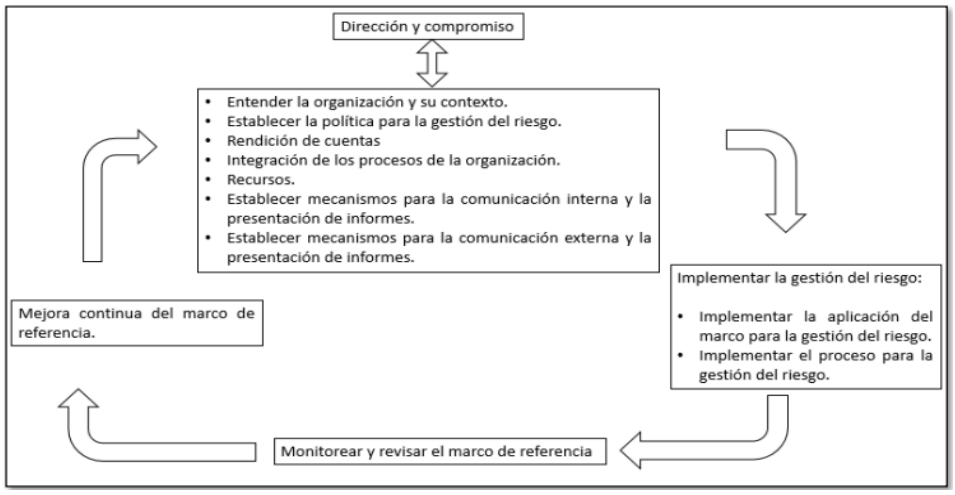
La norma ISO 31000 es una norma desarrollada sobre gestión de riesgos, tiene tres elementos clave, principios, marco y un proceso para la gestión de riesgos. La norma acepta que todas las organizaciones gestionen el riesgo en algún grado, sin embargo, establece los principios que deben cumplirse para que la gestión del riesgo sea efectiva, se recomienda que las organizaciones desarrollen, implementen y mejoren continuamente el marco de referencia, cuyo propósito debe ser integrar los principios y procesos de la gestión de riesgos en todos los procedimientos de la organización. Al implementar los principios y la guía del estándar en una organización, se puede mejorar su eficiencia operativa, gobernanza y confianza de las partes interesadas, y se minimiza cualquier pérdida potencial, esta gestión también debe adaptarse y

alinearse a los perfiles del riesgo, por eso es importante la gestión humana y la información del proceso evaluado.

La norma establece 29 términos y definiciones que dan la guía para realizar una adecuada gestión del riesgo. Esta norma tiene un marco de referencia y un proceso que describen cada punto para tener en cuenta para el éxito de la implementación de la gestión del riesgo en un proceso. Este marco de referencia pretende considerar en todos los niveles de la organización, asegura que la información del riesgo evaluado se reporte adecuadamente, como base para la toma de decisiones, la figura 10 explica la relación de los diferentes componentes del marco.

Figura 10

Marco de gestión del riesgo



Nota. ICONTEC. NTC-ISO 31000:2009

Esta norma menciona que debe incluirse en la cultura organizacional, como parte de la gestión del riesgo en una organización, buscando siempre que los procesos del negocio logren adaptarse a los cambios necesarios para que el riesgo esté controlado.

Como se puede observar en la figura 11 la implementación de la gestión del riesgo es un proceso que se divide en varios pasos, esta gestión comienza:

- Comunicaciones y consultas: Este paso se enfoca en asegurar una comunicación efectiva entre los implicados en los procesos evaluados, considerando tanto actores como internos y externos, para tener definiciones, alcances claros, se considera uno de los pasos a presentar en el proceso, por lo que es transversal en toda la gestión.
- Establecimiento de Contexto: Al establecer el contexto, la organización define tanto los parámetros internos como externos que se tendrán en cuenta a la hora de gestionar el riesgo, también se establecen los criterios para tener en cuenta, es importante que se evalúan con mayor detalle, encontrando la relación específica con el proceso evaluado, así logrando definir el alcance de la gestión a realizar.

  Es importante aclarar que el contexto incluye factores externos como los son social, político, legal, financiero, tendencia de mercado, competencia, etc.; en cuanto al contexto interno hace referencia a misión de la organización, visión, objetivos pretendidos en el proyecto, estructura, colaboradores, funciones específicas, políticas internas, etc.

- Valoración del riesgo: Es el proceso total de la identificación, análisis y evaluación del riesgo en el caso de estudio.

  Se inicia con la identificación de fuentes de riesgo, áreas impactadas, logrando descubrir los eventos o causas que podrían crear, prevenir, acelerar o retrasar el logro del objetivo sea cual sea su origen, con el apoyo de herramientas y técnicas para tener la información actualizada.

  El proceso continúa analizando riesgos, involucra considerar las causas y fuentes del riesgo en sus diferentes grados de detalle, sus consecuencias positivas y negativas,

analizando la posible ocurrencia de estos riesgos, controles aplicables para asegurar su efectividad y eficiencia en la mitigación de riesgos.

En este proceso se incluye la evaluación del riesgo que se enfoca en la toma de decisiones basado en el análisis realizado, identificando los principales riesgos a tratar y su prioridad, consecuentemente se toman decisiones basadas en hasta qué punto se tratará el riesgo y se establece el grado de tolerancia frente a este.

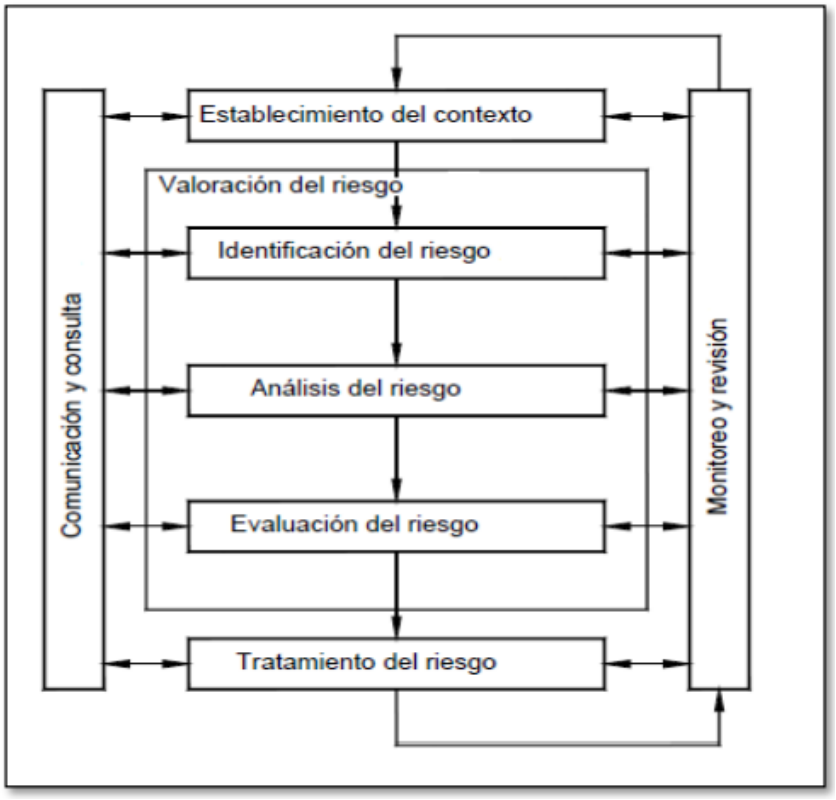
- Valoración del riesgo: El tratamiento se enfoca en la selección de las opciones en las que se enfocarán en modificar los riesgos, como la implementación de estas opciones, esperando como resultado control sobre los mismos.
  Alguno de estos controles tiene diferentes maneras de lidiar con los riesgos, valorando el tratamiento propuesto, tratando los riesgos residuales, tolerancia frente a riesgos tratados o la generación de nuevos tratamientos y la eficacia del tratamiento de los encontrados.
  Para la selección del tratamiento de riesgo como se comentó anteriormente se deben tener en cuenta aspectos legales, reglamentarios, esto enfocado en equilibrar los costos y los esfuerzos relacionados con la mitigación de los riesgos. También se debe tener en cuenta claramente el orden de prioridad de riesgos a tratar, considerando que este tratamiento en sí puede asociarse a nuevos riesgos.

- Monitoreo y revisión: Esta parte debe estar incluida desde el principio del tratamiento del riesgo, puntualmente especificar el quien, cómo, cuándo y dónde se realizarán las verificaciones y vigilancia sobre los tratamientos implementados, garantizando que estos controles o vigilancia sean eficaces en su diseño como en su operación, para brinden

datos que permitan analizar y aprender lecciones, cambios en los ambientes tanto internos como externos y lograr identificar si existen riesgos emergentes.

Figura 11

Proceso de gestión de riesgos.



Nota. ICONTEC. NTC-ISO 31000:2009

Debido a que las ISO 31000 y 27005 no tienen una metodología explicita para gestionar las amenazas de riesgo, por eso y considerando que en el desarrollo de un proyecto presenta riesgos que afectan directa e indirectamente los procesos y sistemas produciendo pérdidas, se deben considerar alternativas para gestionarlos oportunamente. Para dicha propuesta se hará un análisis de estándares, técnicas, metodologías, y buenas prácticas en la gestión de riesgos en las practicas forenses, los resultados servirán de soporte para plantear la gestión de riesgos basada en

las normas ISO 3100 e ISO 27005, una vez que se tenga definida la propuesta, conocer si esta ofrece aportes significativos sobre su implementación en la gestión del riesgo en las practicas forenses de derecho (Mejia-Lobo, 2022).

5.5. Modelo de Seguridad y Privacidad de la Información MSPI.

El Ministerio de Tecnologías y las Comunicaciones de Colombia, desarrollo el MSPI como una estrategia para dicta Lineamientos en entidades del estado, que permita la implementación y adopción en lo referente a la seguridad de la información , adoptando buenas prácticas, tomando como referencia estándares internacionales, que permitan cumplir el objetivo de respecto de la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), que conlleve a la implementación de lo atinente con la Política de Gobierno Digital (MinTIC, 2021).

Teniendo en cuenta lo anterior, el MinTIC elaboró el Modelo de Seguridad y Privacidad de la Información – MSPI y define los Lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de los sujetos obligados un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten que las Entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información. Las fases a las cuales están obligados las Entidades son las siguientes:

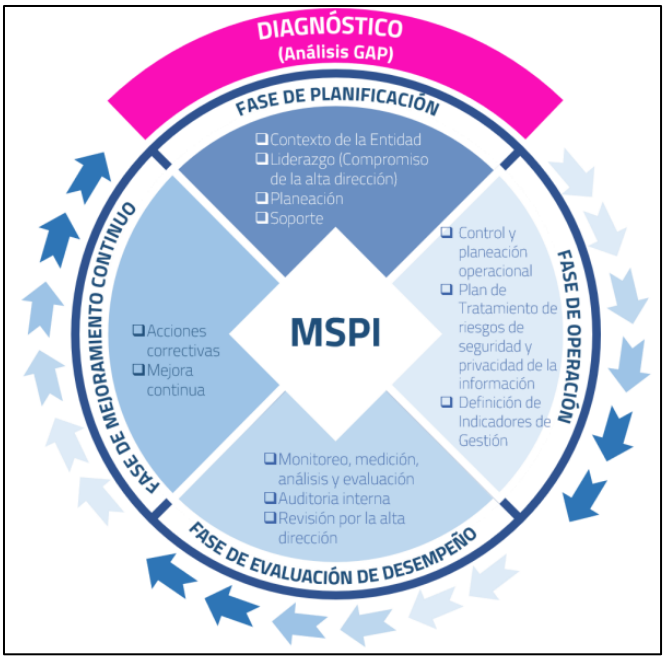
1. **Fase de diagnóstico:** Realizar un diagnóstico o un análisis brechas o GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI. Se

recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 5 de mejora continua.

2. **Fase de planificación: Determinar las necesidades y objetivos de seguridad y privacidad de la información considerando su mapa de procesos, el tamaño y su contexto interno y externo.** Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.
3. **Fase de operación:** Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.
4. **Fase de evaluación de desempeño:** Determinar el sistema y forma de evaluación de la adopción del modelo.
5. **Fase de mejoramiento continuo:** Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

Figura 12

Ciclo del Modelo de Seguridad y Privacidad de la Información.



Fuente: Anexo 01Modelo de Seguridad y Privacidad de la Información

6. Hipótesis de investigación

El diseño del Sistema de Seguridad de la Información para el Instituto de Investigaciones Ambientales del Pacífico, soportado en el MSPI, protegerá los procesos misionales y de apoyo de la entidad, gracias al establecimiento de políticas que ayuden a mitigar los riesgos de la protección de datos, internos y externos.

Razón por la cual la presente Investigación indicará qué controles de seguridad de la información definidos en la norma ISO 27001 y el MSPI, son apropiados para la protección de datos en el IIAP, y que ayuden a mitigar las falencias y posibles causas que inciden en la no prevención de riesgos en términos de:

- Falta de tecnología apropiada en la entidad
- Prácticas no apropiadas en término de uso de las TIC
- No implementación de políticas de seguridad.
- Subestimar los daños que se puedan ocasionar ante a un ataque cibernético.
- La falta de conciencia en la entidad sobre la importancia de los activos de información como un bien intangible.
- Altos procesos manuales.
- Deficiencia respecto de la cultura en seguridad de la información.
- Baja gestión organizacional tecnológica en el IIAP.
- Baja inversión presupuestal en temas relacionados con la seguridad de la información.

7. Metodología

Esta investigación tuvo un enfoque cuantitativo y cualitativo, es decir, mixto, basado en la recolección de datos usando el formato de autoevaluación del Modelo de Seguridad y Privacidad de la Información, teniendo como herramienta de gestión el ciclo PHVA. Adicionalmente el análisis de riesgos se basó en una metodología semicuantitativa, al usar como referentes un análisis de impacto (cuantitativo) y otro cualitativo (probabilidad) más basado en la experiencia.

a. Ciclo PHVA

Es una herramienta de gestión presentada en los años 50 por el estadístico estadounidense Edward Deming, más conocida como el ciclo PHVA (Planificar, Hacer, Verificar y Actuar):

Planificar: En esta etapa se proyectaron los objetivos a alcanzar y se verificaron los procesos vitales que conllevaron a conseguir los resultados acordes a las políticas de la entidad. Igualmente se determinó también los parámetros de medición a ejecutar para el control y seguimiento de los procesos.

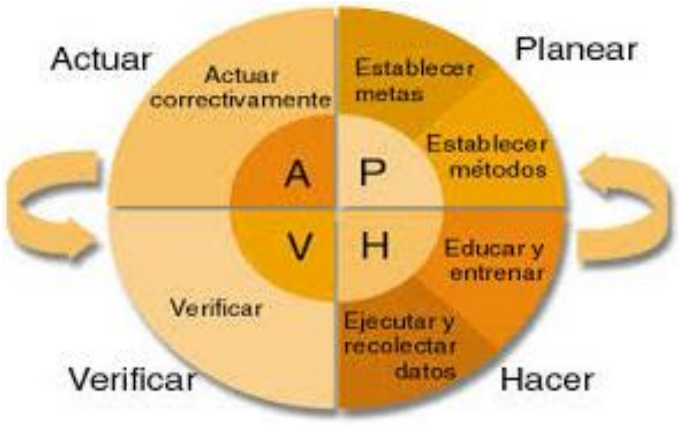
Hacer: Se realizaron cambios o acciones para instaurar las correcciones planificadas. Con el objeto de ser eficaces y poder subsanar ligeramente posibles errores en la ejecución, por lo general se efectuó a un plan piloto a modo de prueba o testeo.

Verificar: Con el plan de mejoras en ejecución, se fijó un lapso de prueba para conocer la efectividad de los cambios procediendo a su medición, que permitió ajustar las correcciones planteadas.

Actuar: Una vez realizada la verificación y ajustes que de no realizarse interferirían con la consecución de los objetivos definidos, se proceden a hacer efectivas dichas correcciones, tomando las medidas adecuadas para optimiza el desarrollo de los procesos. (ISOTOOLS, 2015). Se observa en la figura 12 una imagen del ciclo PHVA:

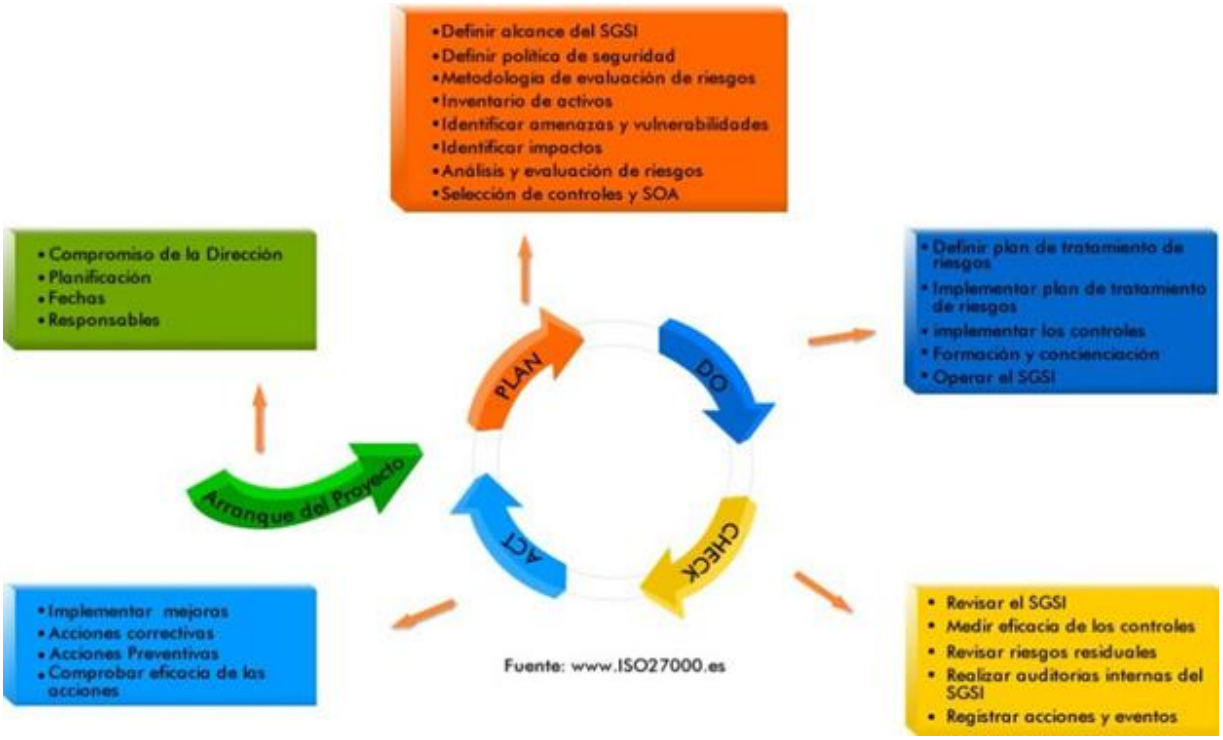
Figura 13

Ciclo PHVA.



Ciclo PHVA para el SGSI

Ciclo PHVA a nivel detallado:



Fuente: www.ISO27000.es

b. Marco MSPI

Asimismo, este ciclo es adoptado por gobierno colombiano al proponer el marco de implementación donde propone 5 fases: Diagnóstico, Planificación, implementación, Gestión y Mejora Continua, donde el presente proyecto aplicado, abarco la fase de planificación del PHVA, que corresponde a la etapa de Diagnóstico y planificación del modelo MSPI, como se observa en la figura 14:

Figura 14

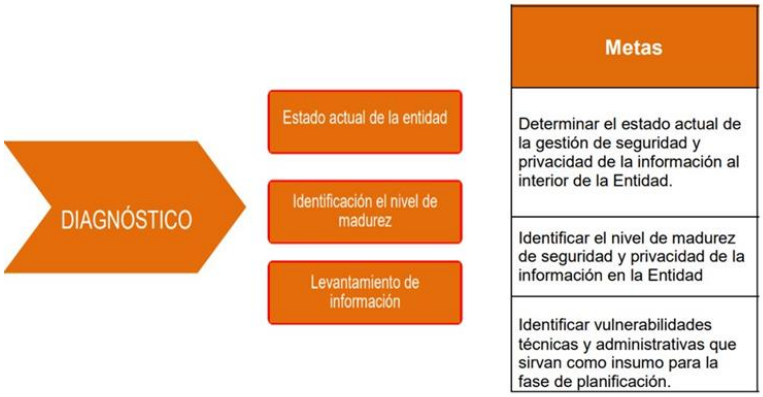
Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información Adaptado del MSPI, MinTIC. (2016).

Fuente: Modelo de seguridad y privacidad de la información, (MinTIC, 2021)

Para la fase de Diagnóstico se tomó la siguiente secuencia según la metodología propuesta por el modelo de seguridad y privacidad de la información del MinTIC, la cual se observa en la figura 15:

Figura 15

Fase de diagnóstico del MSPI



Fuente: Modelo de seguridad y privacidad de la información, (MinTIC, 2021)

Para proceder con el diagnóstico del Instituto de Investigaciones Ambientales del pacifico se procede como primero a identificar el estado actual referente al MSPI, que servirá como punto de partida para determinar políticas y alcances de SGSI en la entidad:

Figura 16

Evaluación de efectividad de controles - ISO 27001:2013 Anexo A

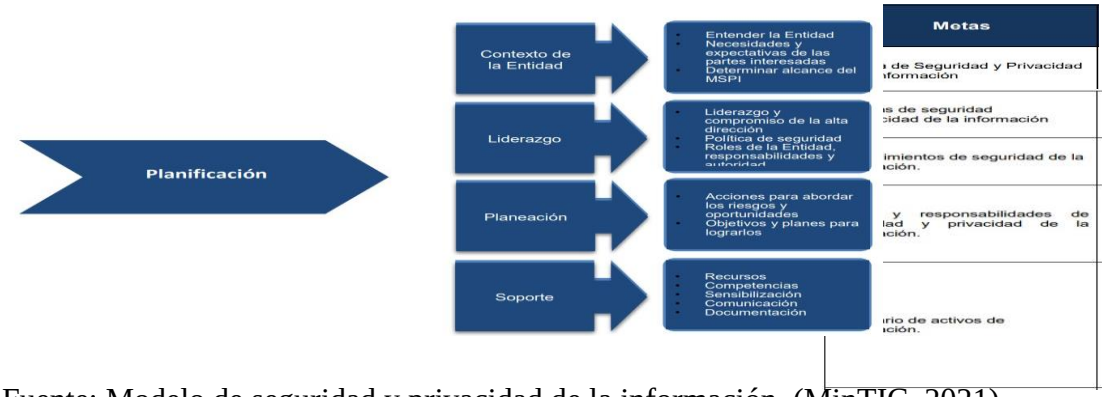
Nota: Resultado de la evaluación de *Evaluación de efectividad de controles - ISO 27001:2013 Anexo A*, MSPI (MinTIC, 2021)

Para el MSPI no se ha actualizado la última versión del estándar 27001:2022, pero que será motivo de recomendaciones en las conclusiones de esta investigación.

Asimismo, para la etapa de planificación se efectúo con base en el modelo mencionado y el cual se refleja en la siguiente figura 17:

Figura 17

Metas Fase de Planeación Adaptado del Modelo de Seguridad y Privacidad de la Información, MinTIC. (2016)



Fuente: Modelo de seguridad y privacidad de la información, (MinTIC, 2021).

Por otra parte, y teniendo en cuenta que el contexto organizacional del MSPI en sí, son las entidades del Estado, la metodología en la cual se basa gestión del riesgo es la guía que propone el Departamento de la Función Pública, DAFP, buscando que haya una integración a lo que se ha desarrollado dentro de la Entidad para otros modelos de Gestión, y de este modo aprovechar el trabajo adelantado en la identificación de Riesgos para ser complementados con los Riesgos de Seguridad.

c. Alcance

El diseño de un sistema de gestión de seguridad de la información para el Instituto de Investigaciones Ambientales del Pacifico, basado en el Modelo de Seguridad y Privacidad de la Información, objeto del presente trabajo de investigación estará enfocado específicamente las fases diseño y planeación, para todos sus procesos resaltando entre ellos los activos de información críticos de los procesos misionales y el proceso TIC, los cuales se resaltan en la figura 18:

Figura 18

Procesos misionales y de apoyo objetos del proyecto

El enfoque principal de este trabajo fue la creación y planificación del Sistema de Gestión de Seguridad de la Información (SGSI) para el IIAP, fundamentado en el Modelo de Seguridad y Privacidad de la Información (MSPI). Esto implicó desarrollar una política de seguridad de la información alineada con el propósito fundamental del IIAP, mediante la identificación y clasificación de sus activos de información. Se determinaron los riesgos a los que se exponen estos activos, evaluando su impacto potencial en la organización, y se propusieron controles para mitigarlos o, si se materializan, contar con mecanismos de contingencia adecuados.

8. Resultados

Los resultados obtenidos en este trabajo de investigación se alinean con los objetivos y metodología planteada, estructurados según las necesidades identificadas en el Instituto de Investigaciones Ambientales del Pacífico, apoyados en los controles de la norma ISO 27001 y las exigencias del Modelo de Seguridad y Privacidad de la información impartido por el MinTIC y que permitirán fortalecer la cultura de seguridad y privacidad, y cumplir la normatividad actual en materia de protección de datos y adelantar un proceso de certificación bajo la norma.

A. Instrumento de identificación de la línea base de seguridad

Tabla 6 Resultado de la Evaluación del MSPI Inicial del IIAP

No.	**Evaluación de Efectividad de controles**			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	Políticas de seguridad de la información	20	100	**INICIAL**
A.6	Organización de la seguridad de la información	15	100	**INICIAL**
A.7	Seguridad de los recursos humanos	16	100	**INICIAL**
A.8	Gestión de activos	37	100	**REPETIBLE**
A.9	Control de acceso	20	100	**INICIAL**
A.10	Criptografía	0	100	**INEXISTENTE**
A.11	Seguridad física y del entorno	22	100	**REPETIBLE**
A.12	Seguridad de las operaciones	10	100	**INICIAL**
A.13	Seguridad de las comunicaciones	3	100	**INICIAL**
A.14	Adquisición, desarrollo y mantenimiento de sistemas	0	100	**INEXISTENTE**
A.15	Relaciones con los proveedores	0	100	**INEXISTENTE**
A.16	Gestión de incidentes de seguridad de la información	3	100	**INICIAL**
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	10	100	**INICIAL**
A.18	Cumplimiento	13,5	100	**INICIAL**
PROMEDIO EVALUACIÓN DE CONTROLES		**12**	**100**	**INICIAL**

Fuente: Anexo A Instrumento de Evaluación del MSPI en el IIAP

B. Política de seguridad de la información para el instituto de investigaciones ambientales del pacífico.

Se logro crear y adoptar la Política General de Seguridad de la Información, la cual fue presentada ante el Comité Administrativo y aprobada por este, siendo firmada por el Director General del IIAP. Esta política se convirtió de obligatorio cumplimiento en todos los procesos y actividades, tanto misionales como de soporte a la gestión.

El documento, disponible en el Anexo B, estableció los objetivos, alcance y disposiciones que comprometen al Instituto de Investigaciones Ambientales del Pacífico a proteger, preservar y gestionar la integridad, confidencialidad, disponibilidad y autenticidad de la información, así como la seguridad digital y la continuidad operativa. Todo esto, de acuerdo con el mapa de procesos y en cumplimiento de los requisitos legales y reglamentarios aplicables.

C. Identificación y clasificación de los activos de información

Como resultado de un trabajo realizado con cada área de la entidad, usando la metodología sugerida y aplicando la recomendada por el Departamento Administrativo de la Función Pública (DAFP) para identificar y clasificar los activos de información, hemos logrado identificar 96 activos en todos los procesos. Es importante destacar que 29 de estos activos tienen una alta criticidad, lo que significa que cualquier violación a ellos podría acarrear consecuencias significativas para el IIAP en términos legales, operativos, de imagen, entre otros aspectos. Se ha proporcionado un resumen de estos activos y su nivel de criticidad en la tabla 7, mientras que los detalles adicionales se pueden encontrar en el Anexo C.

Tabla 7 Resumen activos de información y nivel de criticidad por proceso en el IIAP

PROCESO	**Total activos**	**Criticidad alta**	**Criticidad media**	**Criticidad baja**
Investigación	10	4	1	5
Gestión de la Información y el conocimiento	8	3	0	5
Planeación	7	5	1	1
Jurídica	9	6	1	2
Sistema de gestión	6	2	2	2
Administrativo y financiero	29	14	2	13
Dirección general	3	3	0	0
Control Interno	9	6	1	2
Recurso Humano	7	1	0	6
TIC	10	6	3	1
TOTAL AI	98	50	11	37

Fuente: Anexo C Matriz de identificación clasificación de activos de información del IIAP.

D. matriz de riesgo de seguridad de la información y tratamiento del riesgo en el IIAP

Con base en los resultados de la matriz de activos de información y teniendo presente los 29 activos cuyo impacto es de nivel alto para la entidad, se valoró su nivel de riesgos, que ese encuentra disponible en el Anexo D, de igual manera se procedió a realizar el tratamiento del riesgo y que a continuación se resume en figura 20, mapa de riesgos:

Figura 19

Mapa de Riesgos activos de información impacto alto

IMPACTO							
	Catastrófico	40	Zona de Riesgo Medio 1 Falsificacion de documento (Pt, C)	Zona de Riesgo Medio-Alta 15 Suplantacion, fallas del Software, Acceso ilegal, Actos mal intencionados (Pt, Pc)	Zona de Riesgo Alta 4 Acceso ilegal, Virus informatico (Pv, Pt, C)	Zona de Riesgo Alta	Zona de Riesgo Alta
	Severo	20	Zona de Riesgo Medio-Bajo 4 Acceso ilegal, Fuga de información, falsificacion, Actos malintencionados (Pt, C)	Zona de Riesgo Medio 15 Robo, incendio, Virus informatico, Riesgo legal, Acceso llegal, Falsificaion de documentos (Pv,Pt, C)	Zona de Riesgo Medio-Alta 8 Demora, Virus informatico, Inexactitud, Sabotaje, Acceso ilegal (Pv, Pt, C, R)	Zona de Riesgo Medio-Alta 1 Demora (Pt, C)	Zona de Riesgo Alta
	Grave	10	Zona de Riesgo Medio-Bajo 1 Acceso llegal (Pt, R)	Zona de Riesgo Medio-Bajo 1 Fuga de información (Pv, Pt, Pr)	Zona de Riesgo Medio 1 Inexactitud (Pv, Pt; R)	Zona de Riesgo Medio	Zona de Riesgo Medio-Alta
	Moderado	5	Zona de Riesgo Bajo A	Zona de Riesgo Medio-Bajo	Zona de Riesgo Medio-Bajo	Zona de Riesgo Medio-Bajo	Zona de Riesgo Medio
	Leve	2	Zona de Riesgo Bajo A	Zona de Riesgo Bajo A	Zona de Riesgo Medio-Bajo A	Zona de Riesgo Medio-Bajo	Zona de Riesgo Medio-Bajo
		Frecuencia	Improbable	Remoto	Ocacional	Frecuente	Constante
		Valor	1	2	3	4	5

FRECUENCIA

TRATAMIENTO

A = Asumir o Aceptar el riesgo
Pt = Proteger la empresa o Mitigar el riesgo
E = Evitar el riesgo o Eliminar la actividad
Pv = Prevenir el riesgo
C = Compartir el riesgo
R: Retener el riesgo

Fuente: Anexo D Matriz de Riesgos de activos de información del IIAP.

F. Controles identificados para los riesgos de los activos de información en el IIAP

Tabla 8 Controles ISO/IEC 27002:2022

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
R1	Acceso Ilegal	RM	A 5.18 Derechos de acceso	Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.	A 8.8 Gestión de vulnerabilidades técnicas	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.
R2	Fuga de información y Pérdida de la Confidencialidad	RM	A 8.12 Prevención de fuga de datos	Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.	A 5.32 Derechos de propiedad intelectual	La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.
R3	Virus Informático	RM-A	A 8.7 Protección contra malware	La protección contra el malware se implementará y respaldará mediante la conciencia	A 8.13 Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
				adecuada del usuario.		periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada.
R7	Virus Informático	RM	A 8.7 Protección contra malware	La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.	A 8.13 Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada.
R8	Fallas de Software	RM	A 8.26 Requisitos de seguridad de la aplicación	Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.	A 8.9 Gestión de la configuración	Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.
R13	Falsificación de documentos	RM	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones	A 5.10 Uso aceptable de la información y otros activos asociados	Se identificarán, documentarán e implementarán reglas para el

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
				contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.		uso aceptable y procedimientos para el manejo de la información y otros activos asociados.
R14	Suplantación	RM-A	A 8.5 Autenticación segura	Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.	A 8.7 Protección contra malware	La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.
R15	Fallas de Software	RM-A	A 5.23 Seguridad de la información para el uso de servicios en la nube	Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer de acuerdo con los requisitos de seguridad de la información de la organización.	A 8.13 Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
						tema acordada.
R16	Acceso Ilegal	RM-A	A 8.2 Derechos de acceso privilegiado	La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.	A 8.5 Autenticación segura	Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.
R17	Falsificación de documentos	RM	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.	A 5.10 Uso aceptable de la información y otros activos asociados	Se identificarán, documentarán e implementarán reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.
R18	Falsificación de documentos	RM-A	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones	A 5.10 Uso aceptable de la información y otros activos asociados	Se identificarán, documentarán e implementarán reglas para el

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
				contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.		uso aceptable y procedimientos para el manejo de la información y otros activos asociados.
R19	Actos Malintencionados	RM	A 7.3 Asegurar oficinas, salas e instalaciones	Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones.	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.
R20	Inexactitud	RM-A	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la	A 5.8 Seguridad de la información en la gestión de proyectos.	La seguridad de la información se integrará en la gestión de proyectos.

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
				política de seguridad de la información.		
R21	Falsificación de documentos	RM-A	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.	A 5.10 Uso aceptable de la información y otros activos asociados	Se identificarán, documentarán e implementarán reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.
R22	Fuga de información y Pérdida de la Confidencialidad	RM-A	A 8.12 Prevención de fuga de datos	Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.	A 5.32 Derechos de propiedad intelectual	La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.
R23	Incendio	RM	A 7.5 Protección contra amenazas físicas y ambientales.	Se debe diseñar e implementar la protección contra amenazas físicas y ambientales,	A 8.13 Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
				tales como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.		periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada.
R24	Robo	RM	A 7.2 Entrada física	Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.	A 8.13 Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada.
R25	Riesgo legal	RM	A 5.18 Derechos de acceso	Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del	A 5.3 Segregación de deberes	Deben separarse los deberes y las áreas conflictivos de responsabilidad.

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
				tema de la organización.		
R26	Falsificación de documentos	RM	A 5.33 Protección de registros	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.
R27	Falsificación de documentos	RM-A	A 5.33 Protección de registros	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.
R28	Acceso Ilegal	RM-A	A 5.18 Derechos de acceso	Los derechos de acceso a la información y otros activos	A 8.8 Gestión de vulnerabilidades técnicas	Se debe obtener información sobre las

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
				asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.		vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.
R29	Falsificación de documentos	RM-A	A 5.33 Protección de registros	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.
R30	Acceso Ilegal	RM	A 5.18 Derechos de acceso	Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la	A 8.8 Gestión de vulnerabilidades técnicas	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
				política y las reglas de control de acceso específicas del tema de la organización.		de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.
R31	Acceso Ilegal	RM-A	A 5.18 Derechos de acceso	Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.	A 8.8 Gestión de vulnerabilidades técnicas	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.
R32	Acceso Ilegal	RM-A	A 5.18 Derechos de acceso	Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del	A 8.8 Gestión de vulnerabilidades técnicas	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
				tema de la organización.		medidas apropiadas.
R33	Falsificación de documentos	RM	A 5.33 Protección de registros	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.
R34	Falsificación de documentos	RM	A 5.33 Protección de registros	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
R35	Acceso Ilegal	RM-A	A 8.2 Derechos de acceso privilegiado	La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.	A 8.5 Autenticación segura	Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.
R36	Riesgos Financieros	RM-A	A 5.3 Segregación de deberes	Deben separarse los deberes y las áreas conflictivos de responsabilidad.	A 5.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores	La organización debe monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios.
R37	Falsificación de documentos	RM-A	A 5.33 Protección de registros	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
						hayan cometido una violación a la política de seguridad de la información.
R38	Falsificación de documentos	RM-A	A 5.33 Protección de registros	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.
R39	Virus Informático	RM	A 8.7 Protección contra malware	La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.	A 8.13 Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada.

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
R40	Falsificación de documentos	RM	A 5.33 Protección de registros	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.
R41	Demora	RM-A	5.37 Procedimientos operativos documentados	Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.	A 8.9 Gestión de la configuración	Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.
R42	Demora	RM-A	5.37 Procedimientos operativos documentados	Los procedimientos operativos para las instalaciones de procesamiento de información deben	A 8.9 Gestión de la configuración	Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse,

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
				documentarse y ponerse a disposición del personal que los necesite.		documentarse, implementarse, monitorearse y revisarse.
R43	Actos Malintencionados	RM-A	A 7.3 Asegurar oficinas, salas e instalaciones	Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones.	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.
R44	Acceso Ilegal	RA	A 8.2 Derechos de acceso privilegiado	La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.	A 8.5 Autenticación segura	Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
R45	Virus Informático	RA	A 8.7 Protección contra malware	La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.	A 8.13 Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada.
R46	Actos Malintencionados	RM-A	A 7.3 Asegurar oficinas, salas e instalaciones	Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones.	A 6.4 Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.
R47	Acceso Ilegal	RA	A 8.2 Derechos de acceso privilegiado	La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.	A 8.5 Autenticación segura	Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
						de acceso a la información y la política específica del tema sobre el control de acceso.
R48	Virus Informático	RA	A 8.7 Protección contra malware	La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.	A 8.13 Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada.
R49	Sabotaje	RM-A	A 8.8 Gestión de vulnerabilidades técnicas	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.	A 7.1 Perímetros físicos de seguridad	Los perímetros de seguridad se definirán y utilizarán para proteger las áreas que contienen información y otros activos asociados.

ID	RIESGO	CRITICIDAD DEL RIESGO	CLAUSULA 1 ISO/IEC 27002:2022	CONTROL 1 ISO/IEC 27002:2022	CLAUSULA 2 ISO/IEC 27002:2022	CONTROL 2 ISO/IEC 27002:2022
R50	Acceso Ilegal	RM-A	A 8.2 Derechos de acceso privilegiado	La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.	A 8.5 Autenticación segura	Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.
R51	Virus Informático	RM-A	A 8.7 Protección contra malware	La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.	A 8.13 Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada.

Fuente: Anexo E controles propuestos ISO 27002:2022

F. Declaración de aplicabilidad

Después de realizar el análisis de riesgos correspondiente e identificar los controles, se creó la "Declaración de Aplicabilidad", que revisó los 93 controles sugeridos por la ISO/IEC 27002 y determinó si cada uno de ellos era apropiado para el instituto según los criterios que la ISO/IEC 27001:2022 requiere para garantizar que no se están omitiendo controles y que se proporciona una justificación en caso de que algún control no sea relevante para la empresa. La Tabla 9 muestra el diseño del documento:

Tabla 9: Campos en la declaración de aplicabilidad

CAMPO	DESCRIPCIÓN
Sección	Número de clausula referenciada de la ISO 27001:2022
Objetivo	Objetivo de la Cláusula
Control	Descripción del control
Aplicación	SI: Si es aplicable en la empresa NO: No es aplicable en la empresa
Justificación de exclusión	Justificación del porque se está excluyendo el control
Justificación de inclusión	Criterio para la selección de los controles RL: Requerimientos Legales OC: Obligaciones Contractuales RN/MP: Requerimientos del Negocio/Mejores Practicas RAR: Resultado del Análisis del Riesgo
Adopción	Descripción de cómo se aplicará el control en el IIAP

Fuente: Anexo F Formato declaración de aplicabilidad

9. Conclusiones

Respecto de los objetivos planteados se logró:

Este análisis de seguridad permitió la planificación de sistemas de seguridad y gestión de la información para el Instituto de Investigaciones Ambientales del Pacífico según la norma ISO 27000. Con ello, se puede decir, que está en las primeras etapas de maduración y los resultados de este trabajo reflejan la situación por falta de seguimiento periódico.

De esta forma, las falencias detectadas en todos los niveles de la entidad pueden identificarse más claramente y deben corregirse en el menor tiempo posible. Se puede encontrar, que no cuenta con un mecanismo de comunicación efectivo para divulgar oportunamente los objetivos de planificación del sistema de gestión de la información, las políticas de seguridad de la información y las expectativas basadas en este estándar.

Al integrar toda la información recopilada en el proyecto, es posible mostrar el posible impacto de la indisponibilidad de diversos recursos y considerar la necesidad de desarrollar planes de emergencia, continuidad y desastres; para que la información esté garantizada y protegida. La evaluación de cada uno de los hallazgos encontrados, serán los objetivos más importantes; ya que permitirá determinar causa, efecto y recomendaciones para la empresa.

Se puede observar en la evaluación inicial un patrón de puntajes predominantemente bajos, con la mayoría de los dominios evaluados en el nivel inicial de efectividad. Hay áreas críticas de la seguridad de la información que requieren una mejora significativa, como la criptografía, la

adquisición, desarrollo y mantenimiento de sistemas, y las relaciones con los proveedores, que actualmente están en un estado inexistente.

Aunque algunos dominios muestran una efectividad repetible, indicando que existen procedimientos establecidos y se siguen regularmente, aún hay espacio para mejorar y avanzar hacia un estado más maduro de control. Es esencial priorizar la asignación de recursos y la implementación de medidas correctivas para elevar la efectividad de los controles, especialmente en las áreas identificadas como inexistente o inicial.

La Política General de Seguridad de la Información del IIAP, que se pudo diseñar y aprobar en la realización de este trabajo, esta representa un compromiso sólido y continuo con la protección de los activos de información de la organización. Al establecer estándares claros, roles y responsabilidades definido, la Dirección general del IIAP demuestra su dedicación a garantizar la confidencialidad, integridad y disponibilidad de la información crítica. Sin embargo, el éxito de esta política depende no solo de su implementación, sino también de una cultura organizacional arraigada en la conciencia de seguridad y la colaboración entre todos los miembros del personal. Al mantener un enfoque proactivo en la gestión de riesgos y la adaptación a las amenazas emergentes, el IIAP puede fortalecer aún más su postura de seguridad y seguir siendo un líder en la protección de la información en el contexto de la investigación y el desarrollo en la región del Chocó Biogeográfico.

Con la identificación de los activos de información, su clasificación y valoración se logró evaluar los riesgos asociados a estos y que revela la complejidad y diversidad de las amenazas de

la organización en el panorama actual, en medio de grandes retos respectos de la ciberseguridad. Desde vulnerabilidades técnicas hasta riesgos humanos, el IIAP se encuentra ante una variedad de desafíos que podrían comprometer la confidencialidad, integridad y disponibilidad de sus datos sensibles. Sin embargo, al reconocer estos riesgos y desarrollar estrategias de mitigación adecuadas, el IIAP está en una posición sólida para proteger sus activos de información críticos. Al adoptar un enfoque integral que abarque la tecnología, los procesos y la conciencia del personal, el IIAP puede fortalecer su postura de seguridad y garantizar la continuidad de sus operaciones y cumplimiento de su rol misional.

Esta investigación también deja de presente la necesidad de actualizar el MSPI del MinTIC, por diferentes razones, resaltando que el Modelo de Seguridad y Privacidad de la Información del MinTIC se centra en el sector público colombiano y proporciona directrices específicas adaptadas a este contexto, la ISO 27001:2022 es un estándar más amplio y general que se aplica a cualquier tipo de organización en cualquier país, que para el caso del IIAP por su régimen especial dista un poco de una entidad Publica 100%. De igual manera, resaltar la necesidad de revisar los cambios y actualizaciones de la norma ISO 27001:2022 y que sirvió de apoyo para crear el modelo implementado por las entidades del estado, sobre todo en lo relacionado con los controles y su declaración de aplicabilidad.

10. Recomendaciones

Basándose en los resultados obtenidos y las conclusiones de la investigación sobre el Diseño del Sistema de Gestión de Seguridad de la Información para el Instituto de Investigaciones Ambientales del Pacífico, donde se pudo contrastar el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) con la norma ISO 27001:2022, es evidente la importancia de reconocer las diferencias entre ambos y buscar puntos de integración para asegurar el cumplimiento de ambas normativas y mejorar la implementación propuesta en este trabajo.

En este sentido, se pueden considerar las siguientes recomendaciones:

- Para poder identificar y alinear las brechas entre el MSPI y la ISO 27001:2022, se recomienda hacer un análisis detallado para identificar las áreas donde el Modelo de Seguridad y Privacidad de la Información del MinTIC y la ISO 27001:2022 están alineadas y donde existen brechas. Esto permitirá comprender cómo pueden complementarse mutuamente.
- En el trabajo se pudo llegar identificar que el Modelo del MinTIC y la ISO 27001:2022 comparten principios y metas similares en lo que respecta a proteger la información. Por consiguiente, se aconseja aprovechar estas similitudes para reforzar los sistemas de gestión de seguridad de la información.
- Es recomendable promover la fusión de procesos y controles entre el Modelo de Seguridad del MinTIC y los criterios establecidos en la ISO 27001:2022. Esta medida

garantizará una gestión coherente y eficaz de la seguridad de la información, abarcando tanto los requisitos particulares del MinTIC como los estándares reconocidos a nivel internacional.

- Se recomienda enfáticamente proporcionar formación y capacitación al personal encargado de implementar y mantener tanto el Modelo del MinTIC como la ISO 27001:2022. Esto asegurará que estén familiarizados con los principios y requisitos de ambos sistemas, lo que facilitará su implementación de manera efectiva.
- Se aconseja llevar a cabo auditorías regulares para confirmar el cumplimiento de los requisitos tanto del Modelo del MinTIC como de la ISO 27001:2022, además de identificar posibilidades de mejora continua. De esta manera, se garantizará que los sistemas de gestión de seguridad de la información se mantengan en una evolución constante y en búsqueda de mejoras.

En resumen, la integración estratégica del Modelo de Seguridad y Privacidad de la Información del MinTIC con la ISO 27001:2022 puede establecer un marco sólido y exhaustivo para la gestión de la seguridad de la información. Resulta crucial identificar las sinergias entre ambos sistemas y fomentar su colaboración para asegurar una protección efectiva de la información al interior del Instituto del Instituto de Investigaciones Ambientales del Pacífico.

11. Anexos

Anexo A. Instrumento evaluación MSPI

Esta evaluación inicial proporciona una visión detallada del estado actual de la seguridad de la información en la institución, abarcando 14 dominios críticos definidos por estándares internacionales. Los resultados revelan una situación que requiere atención inmediata y mejoras significativas en casi todos los aspectos de la seguridad de la información. Con una calificación promedio de 12 sobre 100, el IIAP se encuentra en una etapa inicial en la mayoría de los dominios evaluados, lo que indica la necesidad de implementar estrategias robustas para fortalecer su postura de seguridad.

Anexo B. Política general de Seguridad

El Instituto de Investigaciones Ambientales del Pacífico se compromete a proteger, preservar y gestionar la integridad, confidencialidad, disponibilidad y autenticidad de la información, así como la seguridad digital y la continuidad operativa, según lo establecido en el documento, que estableció como política general de seguridad de la información.

Anexo C. Matriz de Inventario y clasificación de activos de información

Esta herramienta fue fundamental en el desarrollo de este trabajo de investigación. Esta matriz proporciona una visión estructurada y detallada de todos los activos de información que posee el IIAP, permitiendo una gestión eficiente y una protección adecuada de los mismos. La matriz incluye campos como el nombre del activo, su descripción, el propietario, la ubicación, la clasificación de confidencialidad, integridad y disponibilidad, así como el valor del activo para la entidad, entre otros.

Anexo D. Matriz de Riesgos de la seguridad de la información

La Matriz de Riesgos de Seguridad de la Información es una herramienta crucial para el Instituto de Investigaciones Ambientales del Pacífico (IIAP) en su misión de proteger datos sensibles y mantener la integridad de sus investigaciones y de igual forma fue de gran ayuda en el trabajo desarrollado. Esta matriz identifica, evalúa y prioriza los riesgos potenciales que podrían comprometer la confidencialidad, integridad y disponibilidad de la información crítica del instituto.

Anexo E. Controles propuestos ISO27002

Se logro identificar una serie de controles de seguridad basados en la norma ISO/IEC 27002:2022 para mitigar los riesgos asociados a sus activos de información. Estos controles abarcan una amplia gama de aspectos, desde la gestión de accesos y la protección contra malware hasta la seguridad física y la prevención de fugas de datos. La tabla presentada detalla los riesgos específicos, su nivel de criticidad y los controles correspondientes de la ISO 27002:2022. Cada riesgo tiene asignados dos controles principales, lo que demuestra un enfoque integral para la seguridad de la información.

Anexo F. Declaración de aplicabilidad

La Declaración de Aplicabilidad es un documento crucial en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). En el caso del resultado obtenido en el Instituto de Investigaciones Ambientales del Pacífico, se destaca que recomienda la adopción de diversos controles organizacionales para garantizar la seguridad de la información. Estos controles abarcan desde políticas de seguridad hasta la gestión de incidentes, pasando por roles y responsabilidades, segregación de deberes, y contacto con autoridades y grupos de interés especial.

12. Referencias Bibliográficas

Aguilar Alonso, I., Carrillo Verdún, J., & Tovar Caro, E. (2017). Description of the structure of the IT demand management process framework. *International Journal of Information Management*, *37*(1), 1461–1473. https://doi.org/10.1016/J.IJINFOMGT.2016.05.004

Aguilar Alonso, I., & Vergara Calderón, J. (2020). Identification of IT Governance Frameworks and Standards Implemented in Organizations. *ICSECC 2020 - 2nd International Conference on Sustainable Engineering and Creative Computing, Proceedings*, 36–41. https://doi.org/10.1109/ICSECC51444.2020.9557561

Arévalo, M. (2022). *ISO 27032, el estándar enfocado en ciberseguridad*. https://www.piranirisk.com/es/blog/iso-27032-el-estandar-enfocado-en-ciberseguridad

Benavides Carranza, J. C. (2019). *Integración de la NTC ISO/IEC 27001:2013 con el Modelo de Seguridad y privacidad de la Información-MSPI del MinTIC*. http://repository.unipiloto.edu.co/handle/20.500.12277/6368

Cano, J. (2012). Seguridad de la información y privacidad: dos conceptos convergentes. *Https://Sistemas.Acis.Org.Co/Index.Php/Sistemas*, 1–9. https://acis.org.co/archivos/Revista/123/Revista%20Sistemas%20Edici%C3%B3n%20123.pdf

Cardona Londoño, A., & Carvajal Portilla, D. L. (2018). *Diseño del sistema de gestión de seguridad de la información basado en la familia de normas de la serie iso/iec 27000 para una entidad pública colombiana*. Https://Repositorio.Autonoma.Edu.Co/. https://repositorio.autonoma.edu.co/bitstream/11182/1003/1/Diseño_sistema_gestión_seguridad_información_basado_familia_normas_serie_ISO/IEC_27000_entidad_pública_colombiana.pdf

Chicano Tejada, E. (2015). *Gestión de incidentes de seguridad informática. IFCT0109 - Ester Chicano Tejada - Google Libros*. https://books.google.com.co/books?hl=es&lr=&id=-04pEAAAQBAJ&oi=fnd&pg=PT3&dq=Gesti%C3%B3n+de+incidentes+de+seguridad+inform%C3%A1tica.+IFCT0109&ots=swIJ5nJsBu&sig=6NcpTptQeFdQzZJm2LKcFszcVmo&redir_esc=y#v=onepage&q=Gesti%C3%B3n%20de%20incidentes%20de%20seguridad%20inform%C3%A1tica.%20IFCT0109&f=false

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal*, *33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202/FULL/PDF

DELOITTE. (2016). *La Evolución de la Gestión de Ciber Riesgos y Seguridad de la Información | Deloitte | Latinoamérica | Riesgo*. https://www2.deloitte.com/hn/es/pages/risk/articles/evolucion-de-la-gestion-de-cyber-riesgos-y-seguridad.html

Equipo TicTac Dirección de desarrollo de programas. (2022). *Estudio trimestral de Ciberseguridad - Ataques a entidades de gobierno*.

Glosario de Términos y definiciones ISO 27000 - ISO 27001. (n.d.). Retrieved September 24, 2022, from https://normaiso27001.es/golsario-de-terminos-y-definiciones-iso-27000/#def32

González Cardona, M. (2021). *Propuesta metodológica para implementar un marco de referencia de gobierno y gestión de las tecnologías de información en las entidades del sector de la economía solidaria de primer nivel de supervisión*. https://repositorio.unal.edu.co/handle/unal/80772

Guardia Palacios, F. (2017). *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN AJUSTADO A LAS NECESIDADES DE LA CORPORACIÓN MÉDICA CLÍNICA VIDA DE QUIBDÓ*. https://repository.upb.edu.co/bitstream/handle/20.500.11912/3567/Dise%C3%B1o%20de%20un%20sistema%20de%20gesti%C3%B3n%20de%20seguridad%20de%20la%20informaci%C3%B3n.....pdf?sequence=1&isAllowed=y

Guzmán-Solano, S. L. (2019). *Guía para la implementación de la norma ISO 27032*. https://hdl.handle.net/10983/23385

Hamdi, Z., Anir Norman, A., Nuha Abdul Molok, N., & Hassandoust, F. (2019). A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors. *Journal of Physics: Conference Series*, *1339*(1), 012103. https://doi.org/10.1088/1742-6596/1339/1/012103

Herramienta de Publicación (IPT) de GBIF. (2023). *IPT*. https://ipt.biodiversidad.co/iiap/

ISO 27001: Vulnerabilidades de la organización. (n.d.). Retrieved February 7, 2023, from https://www.pmg-ssi.com/2015/06/iso-27001-vulnerabilidades-de-la-organizacion/

López Trujillo, M., Marulanda Echeverry, C. E., & Valencia Duque, F. J. (2017). IT GOVERNANCE AND MANAGEMENT IN PUBLIC ENTITIES. *AD-Minister*, *31*, 75–92. https://doi.org/10.17230/AD-MINISTER.31.5

Medina Martínez, J. J., Hernán, C., Osorio, C., & Lobo, M. M. (2021). Análisis del phishing y la ley de delitos informáticos en Colombia. *Cuaderno de Investigaciones: Semilleros Andina*, *1*(14). https://doi.org/10.33132/26196301.1948

Mejia-Lobo, M. (2022). *Software para la gestión de riesgos en las prácticas forenses de derecho basado en los principios de la norma ISO 31000 e ISO 27005. Revista De Ciencias Humanas, Teoría Social Y Pensamiento Crítico*. https://doi.org/10.5281/zenodo.6551136

Mejía-Lobo, M., Hurtado-Gil, S. V., & Grisales-Aguirre, A. M. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista de Ciencias Sociales*, *29*(2), 356–372. https://doi.org/10.31876/RCS.V29I2.39981

Mieres, J. (2009). *Ataques informáticos*. https://www.evilfingers.org/publications/white_AR/01_Ataques_informaticos.pdf

MinTIC. (n.d.). *Normograma del Ministerio de Tecnologías de la Información y las Comunicaciones [RESOLUCION_MINTIC_0500_2021]*. Retrieved November 27, 2023, from https://normograma.MinTIC.gov.co/MinTIC/docs/resolucion_MinTIC_0500_2021.htm

MinTIC. (2011). *Modelo de Seguridad y Privacidad de la Información*. https://www.MinTIC.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MinTIC. (2021). *MinTIC expide la resolución que establece los lineamientos y estándares para la estrategia de seguridad digital*. https://www.MinTIC.gov.co/portal/inicio/Sala-de-prensa/Noticias/162626:MinTIC-expide-la-resolucion-que-establece-los-lineamientos-y-estandares-para-la-estrategia-de-seguridad-digital

MinTIC. (2021). *Modelo de Seguridad y Privacidad de la Información*. https://gobiernodigital.MinTIC.gov.co/seguridadyprivacidad/704/articles-162621_Modelo_de_Seguridad_y_Privacidad__MSPI.pdf

Moreano, R., Jordy, J., Gamboa, A., David, E., Investigación, L. DE, Económico, D., & Emprendimiento, E. (2023). Aplicación de la Norma internacional ISO 27032 para la seguridad de la información en los Marketplace de Facebook, Cusco 2023. *Repositorio Institucional - UCV*. https://repositorio.ucv.edu.pe/handle/20.500.12692/113071

Moscaiza Moncada, O. I. (2018). Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO

27001:2013. *Universidad Peruana de Ciencias Aplicadas (UPC)*. https://repositorioacademico.upc.edu.pe/handle/10757/623063

Navarro, M. (2020). *DISEÑO SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA ORIENT*.

Rojas Suárez, J. P., Vergel-Ortega, M., Pabón Gómez, J. A., Ávila, C., Chinchilla, E. J., & Velásquez Pérez, T. (2019). It governance model for state entities, as support for compliance with the information security and privacy component in the framework of the digital government policy. *Journal of Physics: Conference Series*, *1409*(1), 012005. https://doi.org/10.1088/1742-6596/1409/1/012005

SGSI. (n.d.). Retrieved September 22, 2022, from https://www.iso27000.es/sgsi.html

SIAT-PC. (2023). *SIAT-PC - Sistema de Información Ambiental Territorial del Pacífico*. https://siatpc.co/

Sierra Cubides, M., & Hurtado Castrillón, J. A. (2018). *Modelo de seguridad y privacidad de la información para la alcaldía de Puerto Asís en su fase de diagnóstico y planificación*. https://alejandria.poligran.edu.co/handle/10823/1241

Silva Cuadrado, R., & Jara Velandia, H. Y. (2017). Diseño del modelo de seguridad y privacidad de la información basada en los requerimientos de la estrategia de gobierno en línea para la entidad el fondo pasivo social Ferrocarriles Nacionales de Colombia. *Instname: Universidad Piloto de Colombia*. http://repository.unipiloto.edu.co/handle/20.500.12277/2661

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. https://doi.org/10.1016/J.FUTURE.2018.09.063

Stoll, M. (2018). An information security model for implementing the new ISO 27001. *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications*, *1*, 219–242. https://doi.org/10.4018/978-1-5225-7113-1.CH013

Tristancho, L. A. (2015). ¿POR QUÉ FRACASAN LOS PROYECTOS DE SEGURIDAD DE LA INFORMACIÓN? *Repositorio Universidad Piloto de Colombia*. http://polux.unipiloto.edu.co:8080/00002428.pdf

Valencia Duque, F. J., & Orozco Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Undefined*, *22*, 73–88. https://doi.org/10.17013/RISTI.22.73-88

Vanti, A. A., Solana-González, P., & Seibert, R. (2018). Gobernanza Corporativa y Gobernanza Corporativa de TI utilizando Analytic Hierarchy Process en la creación de valor Corporate Governance and IT Corporate Governance Using the Analytic Hierarchy Process in Creating Value. *Https://Repositorio.Unican.Es/*. https://doi.org/10.17013/risti.27.86-108