Plan Estratégico de Seguridad y Privacidad de la Información

PESI

2024 2027

Secretaría General

Equipo de Sistemas

SGI

1 OBJETIVO

Asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno de la Corporación Autónoma Regional del Atlántico, gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura critica, incidentes de seguridad y la privacidad de la información, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables.

1.1 OBJETIVOS ESPECÍFICOS

- Definir y establecer la Política de Seguridad y Privacidad de la Información de la CRA.
- Definir y establecer las acciones y proyectos necesarios para la implementación efectiva del Modelo de Seguridad y Privacidad de la Información – MSPI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Modelo de Seguridad y Privacidad de la Información.

2 ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar la implementación del Modelo de Seguridad y Privacidad de la Información y los controles del Anexo A de la ISO 27001, implementa lo definido dentro de la Política de Seguridad y Privacidad de la Información, donde se indica que se dará a alcance a todos los procesos de la entidad.

3 DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Decreto 612 de 2018, "*Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado*", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- 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*".

- Capítulo 1 del Título 9 de la parte 2 del Libro 2 *Política de gobierno digital* del Decreto Único Reglamentario del Sector de Tecnologías de la información y las Comunicaciones, Decreto 1078 de 2015 modificado por el Decreto 767 de 2022.
- Manual de Gobierno Digital publicado por MINTIC.
- Modelo de Seguridad y Privacidad de la Información publicado por MINTIC.

4 ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La norma ISO 27001:2013 en su anexo A establece una serie de controles aplicables a los Sistemas de Gestión de Seguridad de la Información basados en este estándar. En la tabla no.1 se muestra el nivel de implementación actual en la entidad de los controles establecidos por dicha norma.

No.	EVALUACIÓN DE EFECTIVIDAD DE CONTROLES			
	Dominio	**Calificación Actual**	**Calificación Objetivo**	**Evaluación de efectividad de control**
A.5	Políticas de seguridad de la información	100	100	**Optimizado**
A.6	Organización de la seguridad de la información	66	100	**Gestionado**
A.7	Seguridad de los recursos humanos	54	100	**Efectivo**
A.8	Gestión de activos	17	100	**Inicial**
A.9	Control de acceso	43	100	**Efectivo**
A.10	Criptografía	30	100	**Repetible**
A.11	Seguridad física y del entorno	53	100	**Efectivo**
A.12	Seguridad de las operaciones	64	100	**Gestionado**
A.13	Seguridad de las comunicaciones	57	100	**Efectivo**
A.14	Adquisición, desarrollo y mantenimiento de sistemas	23	100	**Repetible**
A.15	Relaciones con los proveedores	100	100	**Optimizado**
A.16	Gestión de incidentes de seguridad de la información	60	100	**Efectivo**
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	34	100	**Repetible**
A.18	Cumplimiento	61,5	100	**Gestionado**
Promedio evaluación de controles		**54**	**100**	**Efectivo**

Tabla No.1 Evaluación de efectividad de controles establecidos por el anexo A de la norma ISO 27001:2013

La Figura 1 muestra una representación gráfica de la brecha existente entre los controles actuales de la entidad y el estándar establecido por la norma ISO 27001:2013

Figura No. 1 Brecha entre los controles implementados por la CRA y los controles establecidos por el anexo A de la norma ISO 27001:2013

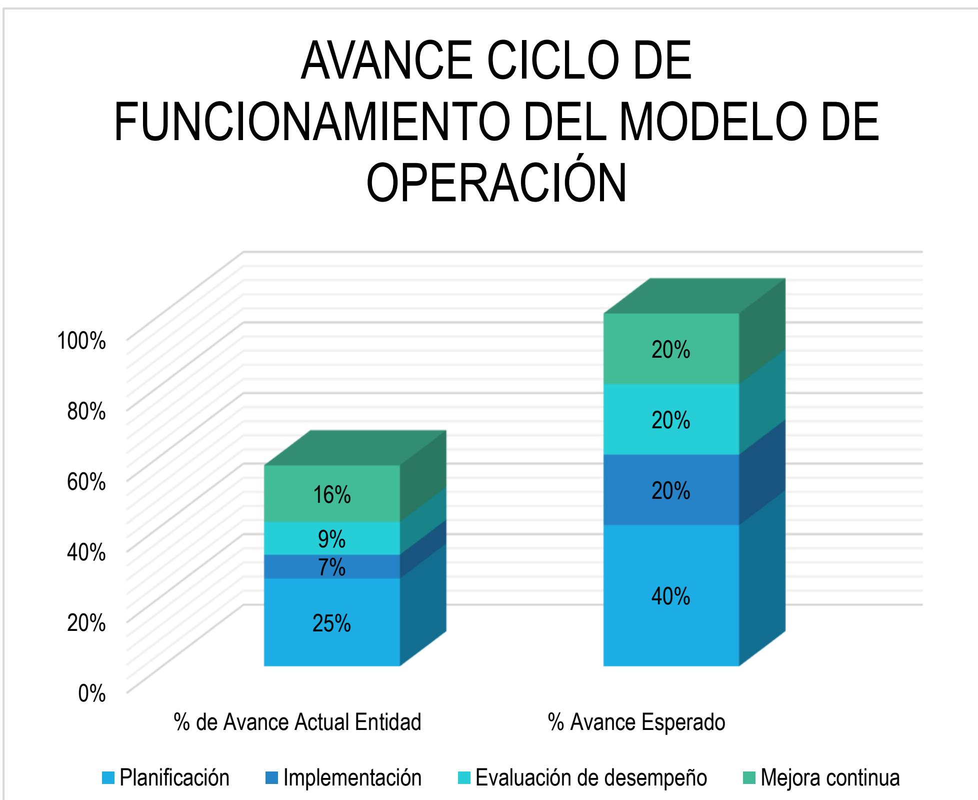


Figura No.2 Representación gráfica del avance en la implementación de los controles del anexo A de la norma ISO 27001:2013 de acuerdo a las fases del ciclo PHVA.

En la figura 2 se muestra la representación gráfica del avance en la implementación de los controles de acuerdo al ciclo PHVA establecido por lo sistemas de gestión, para este caso en específico, el sistema de gestión de seguridad de la información.

Los controles establecidos por el anexo A de la norma ISO 27001:2013 cuentan con la estructura del ciclo PHVA, principio fundamental de sistemas de gestión. Por esta razón es posible analizar los controles de acuerdo a la fase correspondiente del ciclo PHVA, así como se muestra en la tabla 2.

AVANCE PHVA		
COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
Planificación	25%	40%
Implementación	7%	20%
Evaluación de desempeño	9%	20%
Mejora continua	16%	20%
TOTAL	**57%**	**100%**

Tabla No.2 Avance en la implementación de los controles de acuerdo a las fases del ciclo PHVA.

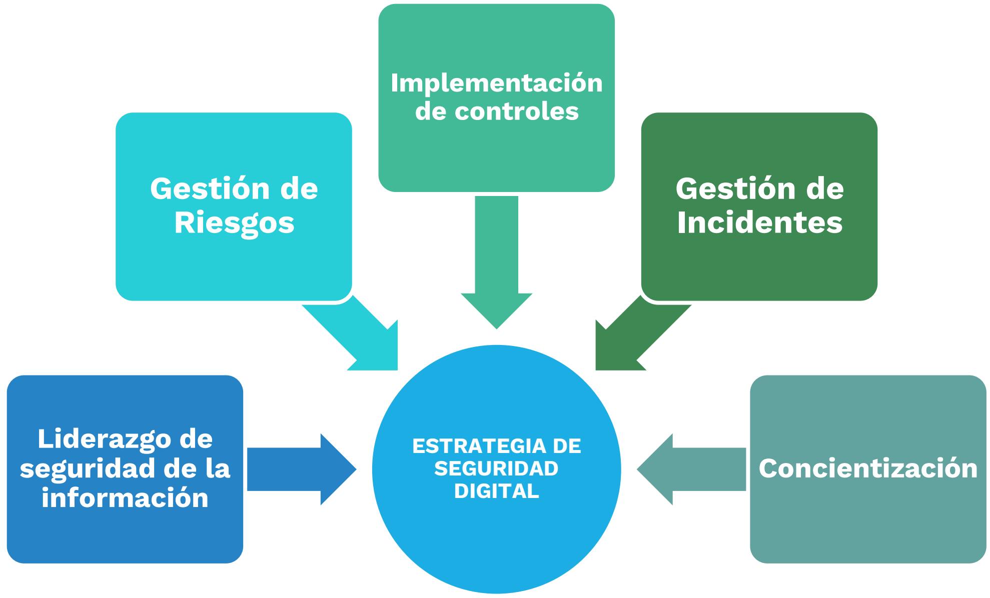
La Corporación Autónoma Regional del Atlántico cuenta con un Sistema de Gestión de la Calidad basado en la norma ISO 9001 desde hace 15 años, hecho que permite mantener una base para la implementación de estándares similares como lo es ISO 27001.

El cumplimiento total del 57% que se muestra en la tabla 2 obedece en gran parte a la estructura que el sistema de gestión de la calidad ha implementado y fortalecido a través de los últimos años. Este hecho resalta la brecha identificada con respecto al cumplimiento del Anexo A de la norma ISO 27001:2013 y demás estándares aplicables como el Modelo de Seguridad y Privacidad de la Información *MSPI* emitido por el Ministerio de Tecnologías de la Información y Comunicaciones *MINTIC.*

5 ESTRATEGIA DE SEGURIDAD DIGITAL

La CRA establecerá una Estrategia de Seguridad Digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse (*Ver Resolución 500 de 2021*).

Por tal motivo, la CRA define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



5.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

5.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, **La Corporación Autónoma Regional del Atlántico** define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
LIDERAZGO DE SEGURIDAD DE LA INFORMACIÓN	Gestión, actualización, comunicación, seguimiento y evaluación de los Planes Estratégicos PETI y PESI	2 planes formulados
	Implementación y certificación en ISO 27001	1 SGSI implementado y certificado con ISO 27001
	Implementación del Modelo de Seguridad y Privacidad de la Información	100% de implementación de los lineamientos del MSPI definido por MinTIC
	Optimización y actualización del Datacenter e implementación de la norma TIA-942	Norma TIA-942 implementada
GESTIÓN DE RIESGOS	Adquisición de certificados, firmas digitales y herramientas de identidad de usuarios y entidad	100% de adquisición de las herramientas y certificados
	Sistema de Backup hibrido para endpoints, servers y Microsoft 365	100% de disponibilidad
	Implementación de sistema de seguridad de acceso físico	1 sistema implementado
	Adquisición de Firewall	2 Firewall adquirido
	Adquisición de Web Acces Firewall	2 Firewall adquirido
CONCIENTIZACIÓN	Construcción e implementación del Plan de fortalecimiento de competencias y habilidades en tecnologías de la información	Capacitación a 100 funcionarios
IMPLEMENTACIÓN DE CONTROLES	Adquisición de herramientas para la gestión de equipos de computo - Gestión de Acceso, Gestión de Identidades y Claves, Mesa de Ayuda, Gestión de Activos de TI, monitoreo de red y Datacenter, monitoreo de endpoints, gestión de eventos-incidentes-problemas.	1 herramienta implementada
	Gestión, monitoreo, análisis, recuperación, continuidad y optimización de los recursos tecnológicos y ciberseguridad	99% de disponibilidad
	Renovación de software base: Acrobat, Adobe Sign, Antivirus Endpoint, Antivirus 365, Vmware, Microsoft 365, Fortinet, Windows (Server y Desktop), Office, Oracle, Acronis, entre otros.	100% de licencias renovadas
	Mantenimiento, soporte, asistencia técnica e instalación de software base para la entidad	1% de indisponibilidad del servicio por vigencia
GESTIÓN DE INCIDENTES	Asistencia técnica y especializada - Mesa de ayuda de nivel III y IV, y gestión de incidentes, problemas y eventos de Tecnologías y Seguridad de la Información	Menos de 5 días en la solución de problemas de nivel I

5.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

El responsable de seguridad de la información, con base a los proyectos definidos en la sección anterior, deberá establecer un cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos. Las actividades podrán desarrollarse de forma secuencial o paralela según se considere.

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS	2024	2025	2026	2027
LIDERAZGO DE SEGURIDAD DE LA INFORMACIÓN	Gestión, actualización, comunicación, seguimiento y evaluación de los Planes Estratégicos PETI y PESI	2 planes formulados	2	0	0	0
	Implementación y certificación en ISO 27001	1 SGSI implementado y certificado con ISO 27001	0	1	0	0
	Implementación del Modelo de Seguridad y Privacidad de la Información	100% de implementación de los lineamientos del MSPI definido por MinTIC	0	1	0	0
	Optimización y actualización del Datacenter e implementación de la norma TIA-942	Norma TIA-942 implementada	0%	0%	50%	50%
GESTIÓN DE RIESGOS	Adquisición de certificados, firmas digitales y herramientas de identidad de usuarios y entidad	100% de adquisición de las herramientas y certificados	100%	100%	100%	100%
	Sistema de Backup hibrido para endpoints, servers y Microsoft 365	100% de respaldo a las máquinas virtuales en producción	100%	100%	100%	100%
	Implementación de sistema de seguridad de acceso físico	1 sistema implementado	0	1	0	0
	Adquisición de Firewall	2 Firewall adquirido	0	2	0	0
	Adquisición de Web Acces Firewall	2 Firewall adquirido	0	2	0	0
CONCIENTIZACIÓN	Construcción e implementación del Plan de fortalecimiento de competencias y habilidades en tecnologías de la información	Capacitación a 100 funcionarios	0	100	100	100
IMPLEMENTACIÓN DE CONTROLES	Adquisición de herramientas para la gestión de equipos de computo - Gestión de Acceso, Gestión de Identidades y Claves, Mesa de Ayuda, Gestión de Activos de TI, monitoreo de red y Datacenter, monitoreo de endpoints, gestión de eventos-incidentes-problemas.	1 herramienta implementada	0	1	0	0

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS	2024	2025	2026	2027
	Gestión, monitoreo, análisis, recuperación, continuidad y optimización de los recursos tecnológicos y ciberseguridad	99,99% de disponibilidad del Datacenter	98%	99%	99,99%	99,99%
	Renovación de software base: Acrobat, Adobe Sign, Antivirus Endpoint, Antivirus 365, Vmware, Microsoft 365, Fortinet, Windows (Server y Desktop), Office, Oracle, Acronis, entre otros.	100% de licencias renovadas	100%	100%	100%	100%
	Mantenimiento, soporte, asistencia técnica e instalación de software base para la entidad	100% de licencias actualizadas	100%	100%	100%	100%
GESTIÓN DE INCIDENTES	Asistencia técnica y especializada - Mesa de ayuda de nivel III y IV, y gestión de incidentes, problemas y eventos de Tecnologías y Seguridad de la Información	Menos de 5 días en la solución de problemas de nivel I	1	1	1	1

6 RESPONSABLES

Se aplicará lo establecido en el documento Modelo de Seguridad y Privacidad de la Información – Roles y Responsabilidades, elaborado por el Ministerio de las TIC. El Director General asignará por resolución las diferentes responsabilidades.

7 APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección y el comité de gestión y desempeño institucional, con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

ELABORÓ		REVISÓ	APROBÓ
Nombre: José Lima Cargo: Profesional Especializado – Secretaría General – TIC	Nombre: Juan Calderón Cargo: Profesional Especializado – Secretaría General – SGI	Nombre: Pedro Cepeda Cargo: Secretario General	Nombre: Jesús León Cargo: Director General Fecha: