



# Plan Estratégico de Seguridad y Privacidad de la Información 2024 – 2027



## 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 crítica, 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



# Plan Estratégico de Seguridad y Privacidad de la Información 2024 – 2027



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.

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES				
No.	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



# Plan Estratégico de Seguridad y Privacidad de la Información 2024 – 2027



EVALUACIÓN DE EFECTIVIDAD DE CONTROLES				
No.	Dominio	Calificación Actual	Calificación Objetivo	Evaluación de efectividad de control
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	34	100	<b>Repetible</b>
A.18	Cumplimiento	61,5	100	<b>Gestionado</b>
<b>Promedio evaluación de controles</b>		<b>54</b>	<b>100</b>	<b>Efectivo</b>

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

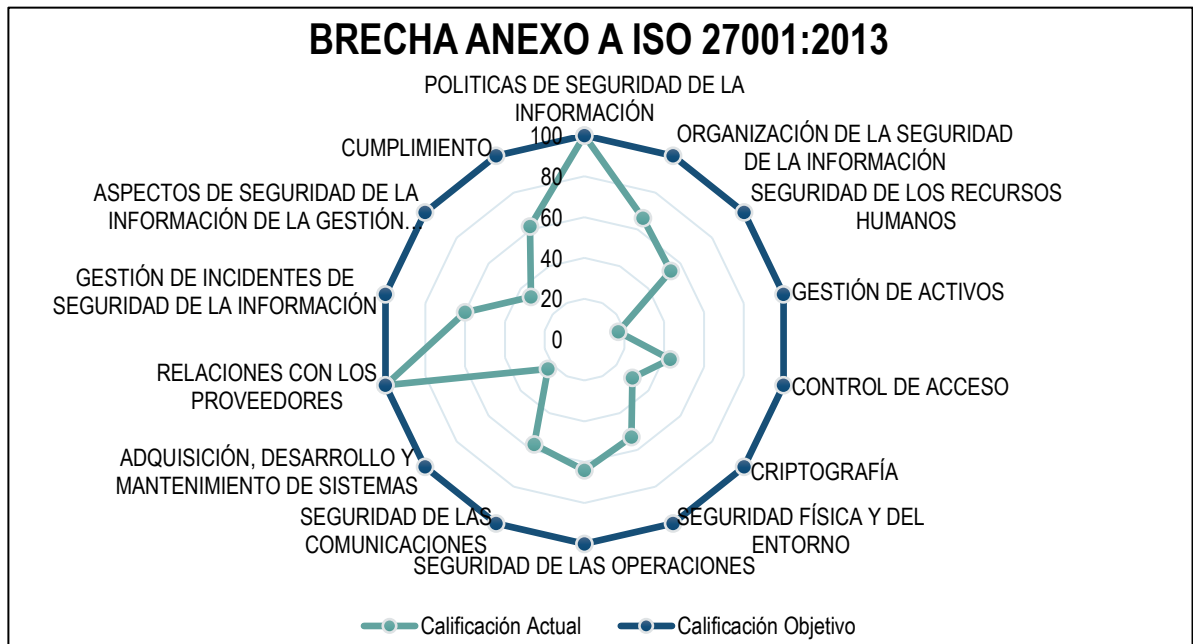


Figura No. 1 Brecha entre los controles implementados por la CRA y los controles establecidos por el anexo A de la norma ISO 27001:2013

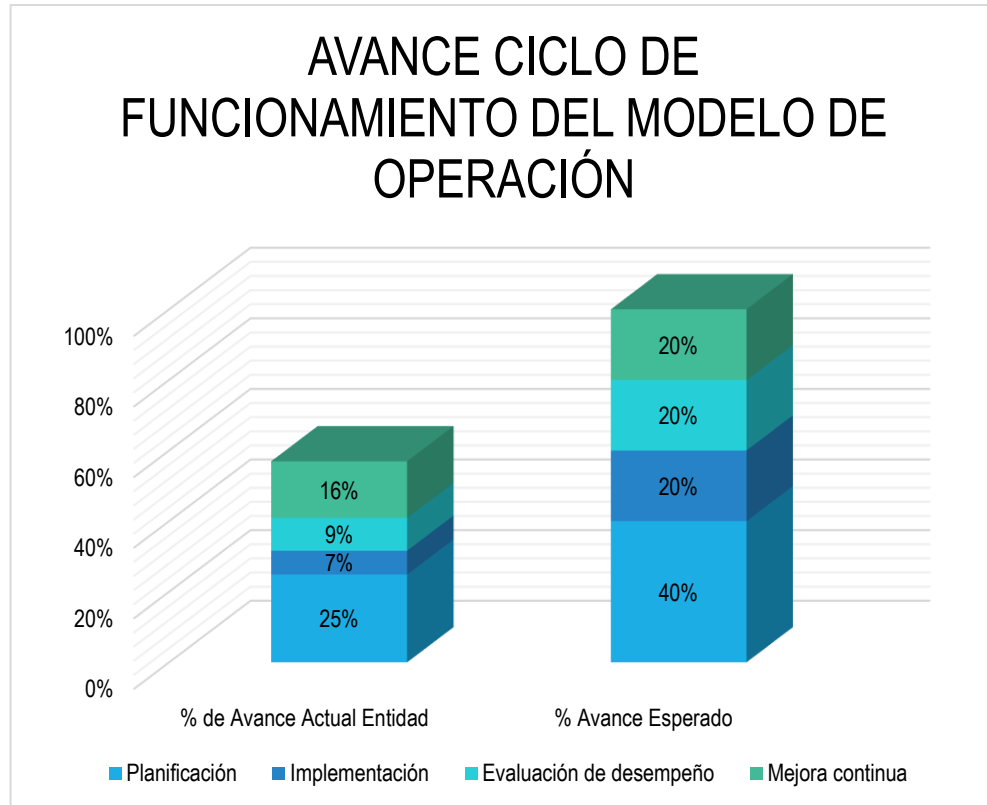


Figura No.2 Representación gráfica del avance en la implementación de los controles del anexo A de la norma ISO 27001:2013 de acuerdo a las fases del ciclo PHVA.

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%
<b>TOTAL</b>	<b>57%</b>	<b>100%</b>

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

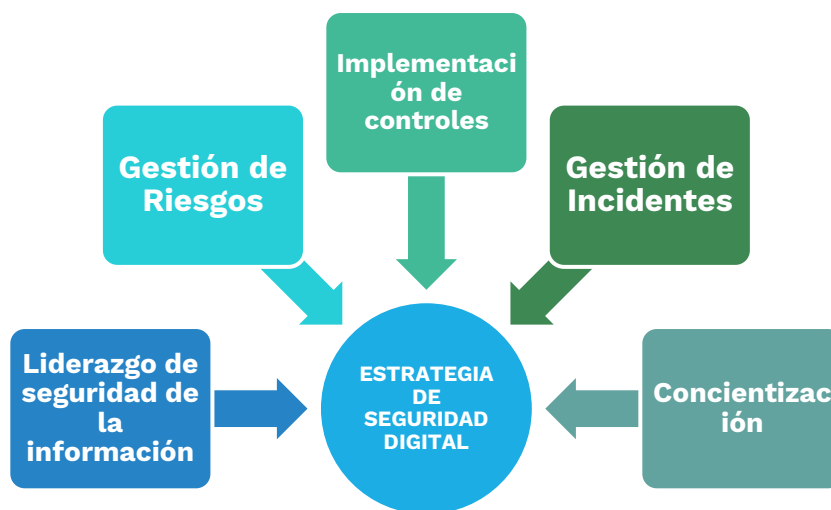
La Corporación Autónoma Regional del Atlántico cuenta con un Sistema de Gestión de la Calidad basado en la norma ISO 9001 desde hace 15 años, hecho que permite mantener una base para la implementación de estándares similares como lo es ISO 27001.

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:





# Plan Estratégico de Seguridad y Privacidad de la Información 2024 – 2027



## 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
<b>Liderazgo de seguridad de la información</b>	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPÍ) 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.
<b>Gestión de riesgos</b>	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.
<b>Concientización</b>	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.
<b>Implementación de controles</b>	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.
<b>Gestión de incidentes</b>	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	ALINEACIÓN PAI
<b>LIDERAZGO DE SEGURIDAD DE LA INFORMACIÓN</b>	Gestión, actualización, comunicación, seguimiento y evaluación de los Planes Estratégicos PETI y PESI	2 planes formulados	6.2.1.1 Revisión de políticas e implementación de lineamientos normativos de la Política de Gobierno Digital.



# Plan Estratégico de Seguridad y Privacidad de la Información 2024 – 2027



ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS	ALINEACIÓN PAI
	Implementación y certificación en ISO 27001	1 SGSI implementado y certificado con ISO 27001	6.7.1.3 Implementar el Sistema de Gestión de Seguridad de la Información bajo la Norma ISO 27001:2022
	Implementación del Modelo de Seguridad y Privacidad de la Información	100% de implementación de los lineamientos del MSPi definido por MinTIC	6.2.2.1 Fortalecimiento de la Seguridad de la Información y Ciberseguridad
	Optimización y actualización del Datacenter e implementación de la norma TIA-942	Norma TIA-942 implementada	6.2.1.1 Garantizar la implementación de lineamientos normativos de la Política de Gobierno Digital.
<b>GESTIÓN DE RIESGOS</b>	Adquisición de certificados, firmas digitales y herramientas de identidad de usuarios y entidad	100% de adquisición de las herramientas y certificados	6.2.2.1 Fortalecimiento de la Seguridad de la Información y Ciberseguridad
	Sistema de Backup híbrido para endpoints, servers y Microsoft 365	100% de disponibilidad	6.2.2.1 Fortalecimiento de la Seguridad de la Información y Ciberseguridad
	Implementación de sistema de seguridad de acceso físico	1 sistema implementado	6.2.2.1 Fortalecimiento de la Seguridad de la Información y Ciberseguridad
	Adquisición de Firewall	2 Firewall adquirido	6.2.2.1 Fortalecimiento de la Seguridad de la Información y Ciberseguridad
	Adquisición de Web Acces Firewall	2 Firewall adquirido	6.2.2.1 Fortalecimiento de la Seguridad de la Información y Ciberseguridad
<b>CONCIENTIZACIÓN</b>	Construcción e implementación del Plan de fortalecimiento de competencias y habilidades en tecnologías de la información	Capacitación a 100 funcionarios	6.2.1.2 Cultura y apropiación digital que desarrollen capacidades para el Acceso, Uso y Aprovechamiento de Tecnologías de la Información
<b>IMPLEMENTACIÓN DE CONTROLES</b>	Adquisición de herramientas para la gestión de equipos de cómputo - 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	6.2.2.1 Fortalecimiento de la Seguridad de la Información y Ciberseguridad



# Plan Estratégico de Seguridad y Privacidad de la Información 2024 – 2027



ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS	ALINEACIÓN PAI
	Gestión, monitoreo, análisis, recuperación, continuidad y optimización de los recursos tecnológicos y ciberseguridad	99% de disponibilidad	6.2.2.1 Fortalecimiento de la Seguridad de la Información y Ciberseguridad
	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	6.2.3.1 Adquisición de Tecnologías de la información
	Mantenimiento, soporte, asistencia técnica e instalación de software base para la entidad	1% de indisponibilidad del servicio por vigencia	6.2.3.2 Mantenimiento, soporte y actualización tecnológica
<b>GESTIÓN DE INCIDENTES</b>	Asistencia técnica y especializada - Mesa de ayuda de nivel II, 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	6.2.3.2 Mantenimiento, soporte y actualización tecnológica

## 5.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

Las actividades se desarrollarán de acuerdo con lo definido en el PAI 2024 – 2027 y el PESI 2024 – 2027.

## 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.





# Plan Estratégico de Seguridad y Privacidad de la Información 2024 – 2027



## 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 González Cargo: Profesional Especializado – Oficina Asesora de Ciencia, Tecnología e Innovación	Nombre: Pedro Cepeda Anaya Cargo: Secretario General	Comité Institucional de Gestión y Desempeño
Nombre: Juan Calderón Beltrán Cargo: Profesional Especializado – Secretaría General – SGI	Nombre: Pamela Lozano Ibañez Cargo: Jefe de Oficina Asesora de Ciencia, Tecnología e Innovación	
05/11/2024	05/11/2024	05/11/2024