PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION: 2025

HISTORIAL DE REVISIÓNES DEL PLAN			
FECHA	**VERSIÓN**	**DESCRIPCIÓN**	**AUTOR**
26/11/2024	1.0	Versión inicial	Álvaro Cárdenas

1. VISIÓN GENERAL

La seguridad y privacidad de la Información como habilitador transversal de la Política de Gobierno Digital se desarrolla a través de la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, alineado con la NTC/IEC ISO 27001:2022, a través de este Plan se busca incorporar y fortalecer la seguridad de la información en todos los procesos, trámites, servicios, sistemas de información e infraestructura del Ministerio de Relaciones Exteriores y su fondo rotatorio, garantizando la Confidencialidad, integridad y disponibilidad de los activos de información.

El Sector de Relaciones Exteriores, en el desarrollo de su estrategia de TI, definió el siguiente objetivo, que se constituye en las directrices a seguir en el Plan Estratégico de Tecnologías de la Información de las entidades que lo conforman: *Desarrollar capacidades en el Sector de Relaciones Exteriores para garantizar la confidencialidad, integridad, disponibilidad y privacidad de los datos, a través de la implementación del proyecto "Implementación del Modelo de Seguridad de la Información para el Sistema de Gestión de Seguridad de la Información, de acuerdo con el estándar ISO/IEC 27001, versión 2022* "

EL Ministerio de Relaciones Exteriores y su fondo Rotatorio definió para el periodo 2023-2026 el siguiente objetivo estratégico: *"Fortalecer integralmente las capacidades de gestión del Ministerio de Relaciones Exteriores y su Fondo Rotatorio para cumplir los objetivos y metas del Gobierno del Cambio. y* en el marco de este objetivo se define la estrategia Transformación digital para la generación de valor público y el mejoramiento del Ministerio de Relaciones Exteriores y su Fondo Rotatorio con la siguiente iniciativa orientada a Seguridad de la Información: "*Fortalecimiento integral del modelo de seguridad y privacidad de la información del Ministerio de Relaciones Exteriores y su Fondo Rotatorio",*

Adicionalmente siguiendo los lineamientos de la Política de Gobierno Digital, reglamentada a través del Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, que en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, y de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información,

Arquitectura y Servicios Ciudadanos Digitales, los cuales permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

De acuerdo con lo estipulado en el numeral 2.1.3 del Manual de Gobierno Digital del MINTIC, el Plan de Seguridad y Privacidad de la Información debe establecer los detalles de cómo se realizará la implementación de la seguridad de la información en los procesos de la entidad, estipulando directrices, tiempo y responsables para lograr un adecuado proceso de gestión, administración, evaluación y resultados del plan desarrollado.

Teniendo en cuenta lo anterior, se formula el presente Plan, en cumplimiento de la normativa aplicable vigente y como parte de los planes institucionales establecidos en el Decreto 612 de 2018.

ARTICULACION ESTRATEGICA:

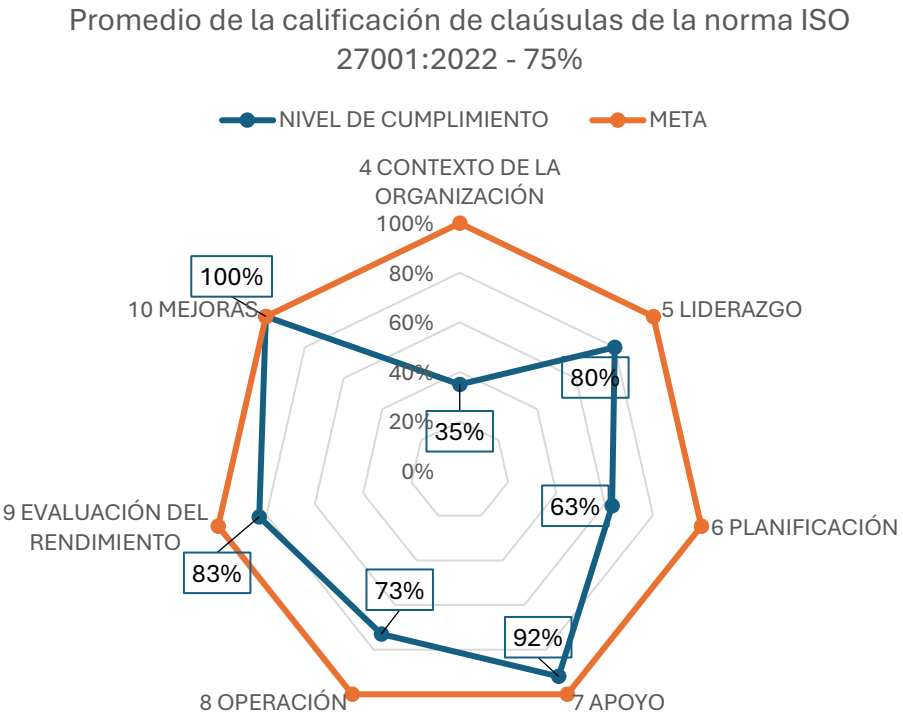
El Plan de Seguridad y privacidad de la información se integra al Plan de Acción Institucional 2025, a través de la siguiente articulación estratégica:

TRANSFORMACIÓN O COMPONENTE	**ODS RELACIONADO**	**PROCESO**	**DIMENSIÓN**	**POLÍTICA**
7. Posicionamiento global y regional de Colombia	16. Paz, justicia e instituciones sólidas	2. Direccionamiento Estratégico	4. Evaluación de Resultados	4.1. Seguimiento y evaluación del desempeño institucional
PLAN	**PROYECTO DE INVERSIÓN**	**OBJETIVO ESTRATÉGICO**	**ESTRATEGIA**	**INICIATIVA**
10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información **12. Plan de Seguridad y Privacidad de la Información**	2.Transformación digital del Ministerio de Relaciones Exteriores	3. Fortalecer integralmente las capacidades de gestión del Ministerio de Relaciones Exteriores y su Fondo Rotatorio para cumplir los objetivos y metas del Gobierno del Cambio.	1. Transformación digital para la generación de valor público y el mejoramiento del Ministerio de Relaciones Exteriores y su Fondo Rotatorio.	Fortalecimiento integral del modelo de seguridad y privacidad de la información del Ministerio de Relaciones Exteriores y su Fondo Rotatorio.

2. SITUACIÓN ACTUAL O DIAGNÓSTICO

De acuerdo con la medición del instrumento de identificación de la línea base de seguridad, ajustado al cumplimiento de la nueva versión de la Norma ISO 27001:2022 y la aplicación del Framework de Ciberseguridad de la NIST, expuesto en el ANEXO 1. Estrategia de Seguridad Digital de este documento, con corte a diciembre

de 2024, el avance general en la implementación del Modelo de Seguridad y privacidad de la Información para los requisitos establecidos en las cláusulas 4 al 10 el de la norma ISO 27001:2022 en el Ministerio de Relaciones Exteriores y su Fondo Rotatorio es del 75%, tal como se presenta a continuación:



Gráfica 1. Promedio de Calificación Cláusulas ISO 27001:2022

El 100% de cumplimiento se alcanzará cuando se logre un nivel Optimizado en el componente de implementación, el cual está relacionado directamente con la implementación de los requisitos establecidos por la norma ISO 27001:2022, y la mejora continua del mismo.

En cuanto al avance en la implementación de los controles del Anexo A de la norma ISO/IEC 27001:2022 el cual posee 93 controles distribuidos en 4 dominios se obtuvieron los siguientes resultados:

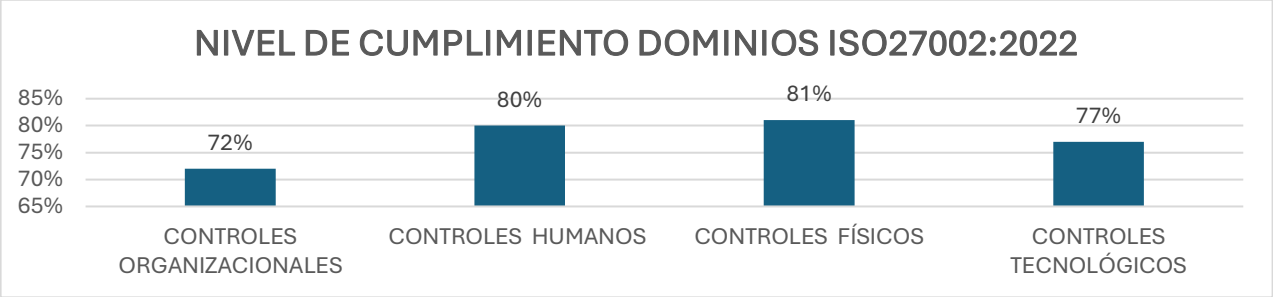


Tabla 1. Nivel Cumplimiento Dominios ISO 27002:2022

Para realizar el comparativo de los controles definidos en la norma ISO 27001:2013 vs ISO27001:2022 se agruparon los controles en las mismas capacidades operacionales que se venían reportando, con el siguiente resultado:

Atributos de Capacidades Operacionales	Diagnostico ISO 27001:2013 AÑO 2023	Diagnostico ISO 27001:2022 AÑO 2024
Gobernanza	100%	100%
Gestión de activos y Protección de la información	83%	60%
Seguridad de los recursos humanos	96%	80%
Seguridad Física	82%	85%
Seguridad de sistemas y redes	86%	88%
Seguridad de aplicaciones	87%	64%
Seguridad Operación Tecnológica	80%	84%
Gestión de identidad y acceso	86%	71%
Continuidad Tecnológica	47%	20%
Seguridad de las relaciones con proveedores	80%	80%
Legal y cumplimiento	91%	77%
Gestión de eventos e incidentes de seguridad de la información	74%	75%
Criptografia	90%	80%
Organización	90%	80%
Nivel de Seguridad	84%	75%

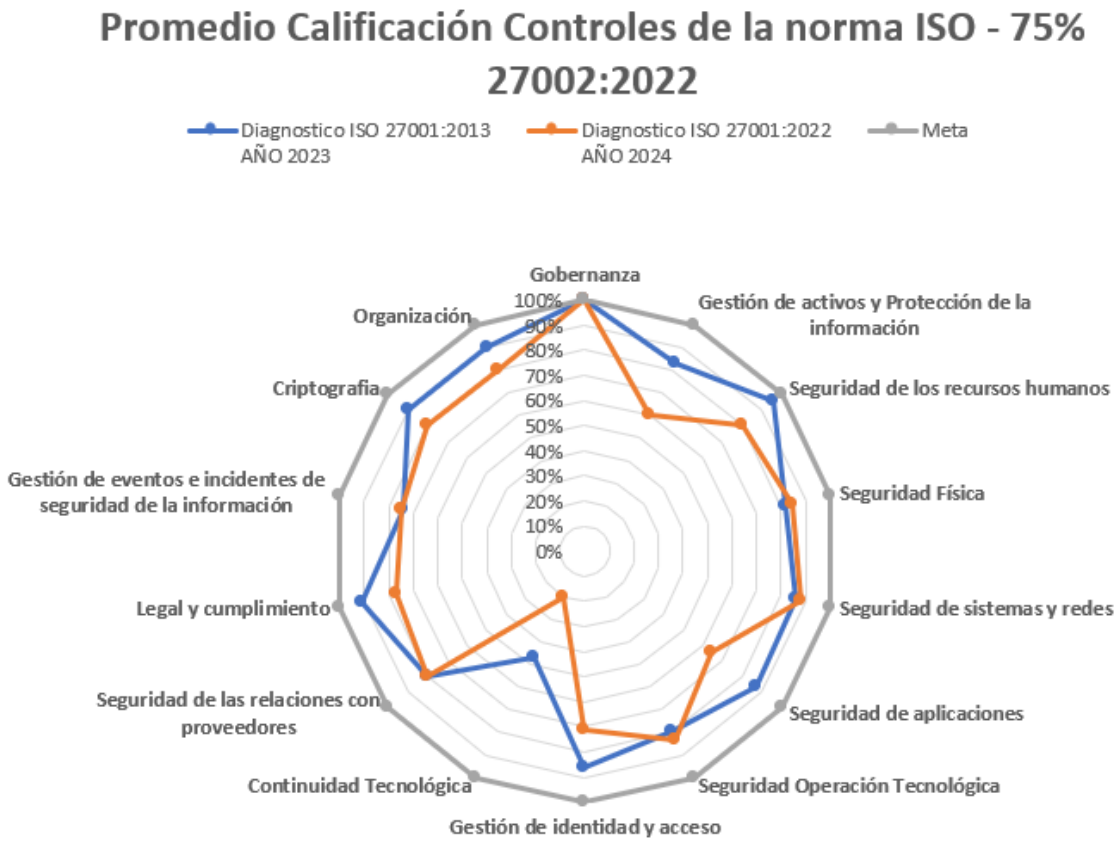
Tabla 2.Comparación Calificación ISO 27001:2013 Vs ISO 27001:2022

Para el cierre del año 2024, se obtuvo una calificación del 75% de avance en la implementación de los controles, esto teniendo en cuenta las acciones ejecutadas en el plan de seguridad y privacidad de la información planeado e implementado en la vigencia 2024.

La valoración realizada de acuerdo con la norma ISO 27001:2022 evidencia una disminución de 9 puntos porcentuales frente al diagnóstico realizado en el año 2023, es necesario aclarar, que esta situación se debe al

cambio de versión de la norma ISO/IEC 27001, la cual incluyó nuevos controles, modificación de algunos y otros eliminados.

A continuación, se muestra gráficamente el resultado del diagnóstico realizado teniendo en cuenta las capacidades operacionales y la nueva medición; por lo que dentro del portafolio de este plan se incluyen actividades que permitirán el fortalecimiento y mejoramiento del sistema de gestión de seguridad de la información, la implementación de los controles nuevos y la mejora continua del sistema.



Gráfica 2. Promedio de Calificación Controles ISO 27001:2022

Del autodiagnóstico realizado se puede concluir:

Los controles que se encuentran en un nivel de implementación inferior al 40%, requieren acciones de reconocimiento, documentación, medición y mejora para llevarlos a un nivel superior, en este nivel se encuentra:

Continuidad Tecnológica

Los controles que se encuentran en un nivel de implementación entre el 40% y 80% se requiere la implementación de acciones de automatización y medición permanente, entre los cuales están:

Gestión de activos y Protección de la información - 60%
Seguridad de aplicaciones - 64%
Gestión de identidad y acceso - 71%
Gestión de eventos e incidentes de seguridad de la información - 75%
Legal y cumplimiento - 77%
Organización - 80%
Seguridad de los recursos humanos - 80%
Seguridad de las relaciones con proveedores - 80%
Criptografia -80%

Los controles que se encuentran en un avance de implementación > 80%, se deben mantener e implementar acciones de monitoreo y medición para garantizar su cumplimiento y actualizados periódica y así lograr el mejoramiento continuo como son:

Seguridad Operación Tecnológica	84%
Seguridad Física	85%
Seguridad de sistemas y redes	88%
Gobernanza	100%

Teniendo en cuenta los anteriores resultados, en la vigencia 2025 se planea llevar a cabo el plan de implementación que se describe en el numeral Cronograma y entregables, todas estas acciones serán lideradas por la Dirección de Gestión de Información y Tecnología – DIGIT, a través del Oficial de Seguridad y privacidad de la Información.

Con la ejecución del cronograma se establecen las actividades a desarrollar en la vigencia 2025, con el fin de avanzar en la implementación del Modelo de Seguridad y Privacidad de la información y obtener una calificación para el 2025 de 85%

3. OBJETIVOS

Definir las acciones, tendientes a fortalecer la seguridad y privacidad de la información del Ministerio de relaciones Exteriores y su Fondo Rotatorio, mediante la planeación de actividades y la implementación de controles de seguridad alineadas con la Norma ISO 27001:2022, la Política de Gobierno y seguridad Digital y el Framework de ciberseguridad de la NIST.

4. ALCANCE

El presente Plan comprende la descripción y programación de las actividades a realizar por el Ministerio de Relaciones Exteriores y su Fondo Rotatorio durante la vigencia 2025, como parte de la implementación del Modelo de Seguridad y privacidad de la información en su última versión y la Estrategia de Seguridad Digital.

5. ESTRATEGIAS, HERRAMIENTAS Y ACTIVIDADES

Dando cumplimiento a la Resolución 500 del Ministerio de Tecnologías de la información y las comunicaciones, la articulación del Plan estratégico de tecnologías de la información, así como la evolución del Marco de Arquitectura Empresarial en el dominio de Arquitectura de seguridad, a continuación, se definen las Estrategias para abordar el avance en la Implementación del Modelo de Seguridad y privacidad de la Información en dos frentes:

Plan de implementación del Modelo de Seguridad y privacidad de la información

La estrategia de Seguridad de la Información se articula con el Ejercicio de Arquitectura empresarial y las brechas identificadas, los frentes de trabajo definidos dentro de esta estrategia buscan cerrar las brechas existentes y avanzar hacia la madurez del modelo de Seguridad y privacidad de la información así:

PROYECTO	ESTRATEGIAS	BRECHAS ARQUITECTURA EMPRESARIAL
PRY-SEG-1.1 Fortalecimiento Integral de la Seguridad: Desarrollo de Controles y Relaciones con Proveedores	**Implementación del Modelo de Seguridad y Privacidad de la Información** Dentro de esta estrategia se encuentran las actividades necesarias para el cumplimiento de las cláusulas 4 al 10 de la norma ISO 27001:2022, la Gestión de Activos y Riesgos de Seguridad de la Información, que incluyen el apoyo a los procesos del Ministerio en la identificación, valoración y definición de acciones de mitigación sobre los riesgos de seguridad y privacidad de la información identificados para los activos con valoración crítica los cuales hacen parte del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Actualización permanente de los activos de información, los cuales se encuentran disponibles para consulta	BreSeg01 BreSeg03 BreSeg05

PROYECTO	ESTRATEGIAS	BRECHAS ARQUITECTURA EMPRESARIAL
	en la página web del Ministerio en el link Registro de Activos de Información | Datos Abiertos Colombia	
	IMPLEMENTACIÓN DE CONTROLES Definición de actividades para la implementación de los controles que se encuentran en estado Inicial, Repetible, Efectivo y Gestionado, los controles que se encuentra en estado optimizado serán monitoreados para garantizar su cumplimiento y actualizados periódicamente para lograr el mejoramiento continuo. La estrategia incluye la definición, monitoreo e implementación de controles organizacionales, físicos, humanos y tecnológicos. Dentro de los controles humanos se incluye la definición y ejecución de una estrategia de sensibilización en Seguridad de la Información y Ciberseguridad con base en la caracterización de grupos focales (Usuarios, Directivos, Técnicos y Terceros), las necesidades de conocimiento en temas de protección de los activos de información, la implementación de mecanismos de protección para la información del Ministerio, así como, el conocimiento en tendencias de ciberseguridad, la cual se encuentra definida en el plan de Sensibilización en seguridad y privacidad de la información	BreSeg02 BreSeg03 BreSeg04 BreSeg07
	GESTIÓN DE PROYECTOS PARA LA IMPLEMENTACIÓN DE LA ESTRATEGIA DE SEGURIDAD DIGITAL A través de la adquisición o contratación de servicios de seguridad y Ciberseguridad para mejorar la postura y monitoreo de seguridad del Ministerio	BreSeg06 BreSeg02 BreSeg07 BreSeg09 BreSeg10

La Estrategia de Seguridad Digital y Ciberseguridad

Como parte de los proyectos establecidos en el Plan estratégico de tecnologías de la información PETI vigencia 2023-2026, y de acuerdo con el Ejercicio de Arquitectura empresarial desarrollado en la vigencia 2023, dentro del dominio de Seguridad, se estableció el desarrollo del Programa de Fortalecimiento de la seguridad y aspectos

asociados, Proyecto PRY-SEG-1.1 Fortalecimiento Integral de la Seguridad: Desarrollo de Controles y Relaciones con Proveedores, como se muestra en la tabla anterior permite el cierre de la brecha de seguridad del ejercicio de Arquitectura Empresarial, En el Anexo 1 de del presente documento se muestran el resultado de la evaluación realizada frente al cumplimiento del Framework de Ciberseguridad de
la NIST, y las acciones a desarrollar dentro de la hoja de ruta de arquitectura de Seguridad a corto mediano y largo plazo.

ESTRATEGIAS DE SEGURIDAD DIGITAL Y CIBERSEGURIDAD					
NIST	**Estrategia**	**Tecnologías y/o Procesos**	**Corto Plazo**	**Mediano Plazo**	**Largo Plazo**
Identificar	Existe un procedimiento de vulnerabilidad y Riesgo se debe mejorar	Programa de Vulnerabilidad con proveedor con apoyo de correlación			**X**
	Programas de sensibilización en ciberseguridad a funcionarios	Realizar ejercicio de Phishing controlados, generar cursos o boletines de usted depende	**X**		
	Matriz de Roles y Responsabilidades	Mantener Actualizado el Árbol telefónico y definir roles entre los funcionarios y contratistas Aliados de tecnología	**X**		
	Matriz de Clasificación de aplicaciones	Mantener actualizado el mapa de aplicaciones con alto Riesgo e identificar Respaldos para una recuperación temprana y crear una Matriz de recuperación activos críticos	**X**		
	Inventario de equipos	Procedimiento de inventario de los dispositivos de la organización		**X**	
Proteger	Autenticación de 2FA en aplicaciones	Extender solución de 2FA a las aplicaciones críticas del Ministerio (Vpn ssl, páginas Web)	**X**		
	Implementar solución de WAF	Aplicar solución de WAF en todas las soluciones WEB expuestas a Internet	**X**		
	Mejorar control de Acceso Redes LAN WIFI	Mecanismos de control de acceso a la red LAN y WLAN basados en identidad, tipo de dispositivo o perfil de riesgo que esté presente		**X**	
	Herramientas que protejan a la organización de usuarios externos por VPN	Implementación de solución ZTNA Para extender protección de equipos remotos			**X**

ESTRATEGIAS DE SEGURIDAD DIGITAL Y CIBERSEGURIDAD					
NIST	**Estrategia**	**Tecnologías y/o Procesos**	**Corto Plazo**	**Mediano Plazo**	**Largo Plazo**
	Protección de Datos en tránsito (conexiones con terceros, usuarios finales, conexión a la nube) están protegidos en cuanto a disponibilidad (redundancia) y confidencialidad de la información (Cifrado de canales)	Implementar Cifrado en la Nube con aliados o terceros con arquitectura de DRP			**X**
	Usar herramientas de protección para aplicaciones web internas, externas y en la nube basados en tecnología avanzada de ML e inspección de comportamientos	Fortalecer la Solución de XDR para validación de comportamiento de los equipos o movimientos laterales	**X**		
	Protecciones contra fugas de datos en el correo, endpoints y perímetro	Implementar DLP en correos soluciones de chat corporativas y sistemas de SharePoint			**X**
Detectar	Usar herramienta de anti-ransomware o sandbox	Implementar soluciones con Sandbox para validación de archivos malintencionados			**X**
	Actualizar la operación con herramientas de correlación de eventos SIEM	Implementar herramienta de correlación SIEM	**X**		
	Mejora los procesos y herramientas de monitoreo de disponibilidad y seguridad que permitan tener una postura menos reactiva y más proactiva de seguridad	Implementar una solución de monitoreo con un contratista a nivel de SOC Y NOC con uso de SOAR	**X**		
	Considerar el uso de herramientas de señuelos para que permita detectar comportamientos anómalos para su análisis y posterior remediación	Implementar opciones de señuelos para validar tráfico malintencionado en soluciones web		**X**	
	Proceso de prueba periódico de los controles de ciberseguridad y procesos de detección y monitoreo de la red	Implementar ejercicios de intrusión a lineados a la NIST 800-53 por lo menos una por semestre		**X**	
Responder	Mejorar el plan de respuesta con alternativas de automatización y respuesta a incidentes de Seguridad	Implementar casos de uso para automatización de eventos respetivos y descartar falsos positivos de las herramientas de ciberseguridad			**X**

ESTRATEGIAS DE SEGURIDAD DIGITAL Y CIBERSEGURIDAD					
NIST	**Estrategia**	**Tecnologías y/o Procesos**	**Corto Plazo**	**Mediano Plazo**	**Largo Plazo**
	Mantener actualizada la matriz de responsables con un debido proceso de comunicación.	Mejorar el proceso de escalamiento y disponibilidad del personal interno como contratistas		**X**	
	Planes de respuesta (respuesta ante incidentes y continuidad del negocio) y los planes de recuperación (recuperación ante incidentes y recuperación ante desastres) están implementados y gestionados	Implementar pruebas por lo menos una vez por semestre al plan de recuperación y continuidad de negocio, validar funcionamiento de replicaciones y alta disponibilidad de Activos críticos de la institución			**X**
Recuperar	Mecanismos de Resiliencia para Servicios críticos, Sedes, Datacenter y soluciones en la Nube	Implementar Soluciones de DRP(para aplicaciones críticas, para Datacenter principal y sedes(con canales de Datos e Internet con alta Disponibilidad, para soluciones en la Nube utilizar Replicaciones en los nodos disponibles contratados			**X**

Las actividades que harán parte de la Estrategia de Seguridad Digital para la vigencia 2025 se encuentran definidas en el Numeral 7. Cronograma y Entregables.

6. PRESUPUESTO

El presupuesto para la implementación del plan de Seguridad y Privacidad de la información será:

AÑO 2025	
PROYECTO	**Inversión**
Objetivo 3: Implementar un modelo de Seguridad y Privacidad de la información. Producto 3.1 Documentos de política - Modelo de políticas y lineamientos de Seguridad y Privacidad de la Información Certificación ISO	$ 2.800.000.000

7. CRONOGRAMA Y ENTREGABLES

Para el seguimiento al cumplimiento de la Estrategia, el Ministerio ha definido las siguientes actividades que tiene por objetivo lograr la implementación y mejoramiento continuo del Modelo de Seguridad y Privacidad de la información:

Para efectos de entendimiento del Cronograma las siglas utilizadas obedecen a:
OSI - Oficial de Seguridad de la Información
GSI - Grupo de Sistemas de Información
GST- Grupo de Servicios Tecnológicos
GGT - Grupo de Gobierno de Tecnologías de la Información

ESTRATEGIA	ACTIVIDADES	RESPONSABLE	FECHAS DE PROGRAMACION	
			FECHA INICO	FECHA FINAL
IMPLEMENTACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	**CLAUSULAS ISO 27001:2022**			
	1. Tramitar la publicación de los instrumentos de gestión pública para dar cumplimiento a la ley 1712 en la página web y portal de datos abiertos	OSI	ENERO DE 2025	FEBRERO DE 2025
	2. Apoyar a los procesos en la identificación de los riesgos y la implementación de los controles de seguridad de la información y la entrega para consolidación en la matriz de riesgos institucional	OSI	ENERO DE 2025	DICIEMBRE DE 2025
	3. Actualizar la documentación del SGSI que se requiera, y realizar la inclusión de los controles de seguridad	OSI	ENERO DE 2025	DICIEMBRE DE 2025
	4. Realizar el autodiagnóstico del Modelo de Seguridad y privacidad de la información	OSI	OCTUBRE DE 2025	DICIEMBRE DE 2025
	5. Realizar la actualización del plan de seguridad y privacidad de la Información	OSI	OCTUBRE DE 2025	DICIEMBRE DE 2025
	6. Realizar la actualización anual del registro de activos de información con cada una de las áreas.	OSI	OCTUBRE DE 2025	DICIEMBRE DE 2025
	7. Definir, presentar para aprobación y publicar el plan de tratamiento de riesgos de seguridad y privacidad de la información y el Plan de Seguridad y privacidad de la información	OSI	OCTUBRE DE 2025	DICIEMBRE DE 2025

ESTRATEGIA	ACTIVIDADES	RESPONSABLE	FECHAS DE PROGRAMACION	
			FECHA INICO	FECHA FINAL
IMPLEMENTACIÓN	**CONTROLES HUMANOS**			

	1. Definir el plan de Sensibilización de Seguridad de la información y ciberseguridad para la vigencia 2025	OSI – GG	ENERO DE 2025	FEBRERO DE 2025
	2. Ejecutar el Plan de Sensibilización definido	OSI – GGT	ENERO DE 2025	DICIEMBRE DE 2025
	3. Establecimiento de la guía ara el uso aceptable de los activos de información en el proceso de talento humano	OSI – GGT	ENERO DE 2025	DICIEMBRE DE 2025
	4. Establecer los lineamientos y el procedimiento para la gestión de los equipos de cómputo, propios de terceros y alquilados	OSI - GGT	MARZO DE 2025	JUNIO DE 2025
	CONTROLES ORGANIZACIONALES			
	1. Construir los procedimientos para la gestión de perfiles	OSI	ENERO DE 2025	DICIEMBRE DE 2025
	2. Realizar el levantamiento de perfiles y roles de todos los procesos para las aplicaciones y sistemas de información	OSI	ENERO DE 2025	DICIEMBRE DE 2025
	3. Implementar el procedimiento de gestión de los perfiles	OSI	OCTUBRE DE 2025	DICIEMBRE DE 2025
	4. Construir el flujo de aprovisionamiento de usuarios	OSI	OCTUBRE DE 2025	DICIEMBRE DE 2025
	5. Desarrollar la estrategia para el etiquetado de la información clasificada	OSI	ENERO DE 2025	DICIEMBRE DE 2025
	6. Definir la estrategia para el cumplimiento de la política de control de acceso	OSI	ENERO DE 2025	DICIEMBRE DE 2025
	7. Definir las guías de atención para los incidentes comúnmente presentados	OSI	ENERO DE 2025	DICIEMBRE DE 2025
	8. Realizar la definición de los planes de contingencia de la infraestructura tecnológica	OSI	ENERO DE 2025	DICIEMBRE DE 2025
	9. Apoyar la implementación de la Estrategia de Continuidad del negocio de acuerdo con el BIA definido por la Oficina de Asesora de Planeación	OSI	JUNIO DE 2025	DICIEMBRE DE 2025
	CONTROLES FISICOS			
	1. Diseñar en conjunto con el GIT de servicios tecnológicos la estrategia para la asignación de Equipos que incluya el software y aplicaciones base de los equipos y las políticas de seguridad (medios, almacenamiento, mantenimiento eliminación)	OSI - GST	MAYO DE 2025	DICIEMBRE DE 2025
	CONTROLES TECNOLOGICOS			
	1. Validar y apoyar las pruebas de restauración de respaldos	OSI - GST	JUNIO DE 2025	DICIEMBRE DE 2025
	2. Hacer Seguimiento al cierre de brecha de la implementación del anexo 3 de la resolución 1519 de 2021	OSI - GSI	ENERO DE 2025	DICIEMBRE DE 2025
	3. Actualización de políticas y principios de desarrollo seguro de software	OSI- GSI	ENERO DE 2025	DICIEMBRE DE 2025

	4. Implementar controles de código fuente, gestión de requerimientos y gestión de pruebas	OSI-GSI	ENERO DE 2025	DICIEMBRE DE 2025
	5. Realizar reportes de revisión de código seguro.	OSI-GSI	ENERO DE 2025	DICIEMBRE DE 2025
	6. Actualización de los planes de contingencia tecnológica	OSI - GST	ENERO DE 2025	DICIEMBRE DE 2025
	7. Actualización Planes de recuperación ante desastres (DRP)	OSI - GST	ENERO DE 2025	DICIEMBRE DE 2025
	8. Realizar el proceso de aseguramiento de los sitios que requieran autenticación a través de certificados digitales	OSI - GST	ENERO DE 2025	DICIEMBRE DE 2025
	9. Realizar el proceso para la adquisición de los certificados y firmas digitales que se requieran para la operación.	OSI - GGT	ENERO DE 2025	DICIEMBRE DE 2025
	10. Seguimiento a la aplicación de controles criptográficos para la protección de la información	OSI - GST	ENERO DE 2025	DICIEMBRE DE 2025

ESTRATEGIA	ACTIVIDADES	RESPONSABLE	FECHAS DE PROGRAMACION	
			FECHA INICO	FECHA FINAL
Gestión de Proyectos para la Implementación de la Estrategia de Seguridad Digital	**CENTRO DE OPERACIONES DE SEGURIDAD – SOC-NOC**			
	1. Adquisición de herramienta de Correlación de Eventos de Seguridad	OSI - GST	ENERO DE 2025	DICIEMBRE DE 2025
	2. Adquisición de Servicios de Monitoreo y respuesta a Incidentes de Seguridad de la Información incluye: • Integración para el monitoreo y análisis de vulnerabilidades • Análisis inteligente de Amenazas • Servicios y herramientas para la automatización, prevención y respuesta contra ciberataques. SOAR • Integración para el Análisis de código Malicioso • Pruebas de vulnerabilidad Ethical Hacking (OWASP) • Monitoreo de Marca	OSI - GST	ENERO DE 2025	DICIEMBRE DE 2025
	2. Adquisición de Servicio de Monitoreo de la Capacidad y Disponibilidad de la Infraestructura tecnológica -NAC	OSI - GST	ENERO DE 2025	DICIEMBRE DE 2025

8. RIESGOS

RIESGO	PROBABILIDAD	IMPACTO	CONTROL PROPUESTO
Disponibilidad de recursos: La falta de recursos necesarios, como personal capacitado, equipos o materiales, puede retrasar o incluso detener la ejecución del plan de seguridad	MEDIA	ALTO	Se debe asegurar la contratación del personal requerido para ejecutar las actividades definidas en el Plan
Gestión de recursos: Una mala gestión de los recursos, como la asignación ineficiente o la falta de coordinación entre equipos, puede llevar a sobrecargas de trabajo, errores y fallos en la implementación del plan	BAJA	ALTO	Se debe realizar una correcta coordinación del tiempo, alcance, y personas capacitadas para la ejecución de las actividades del plan
Costos de recursos: Los costos inesperados o el aumento en los precios de los recursos pueden afectar el presupuesto del plan, limitando la capacidad para implementar todas las medidas de seguridad	MEDIO	ALTO	Se debe realizar un análisis previo de los requerimientos técnicos asociados a los procesos de contratación a través de acuerdos que garanticen los mejores precios.

Nota: Medir Probabilidad e Impacto en: Alto, Medio, Bajo.

9. MEDICIÓN DE RESULTADOS

La medición se realiza con el indicador “Cumplimiento en la implementación del Plan de Seguridad”, que está orientado principalmente a aumentar el nivel de madurez de la implementación y operación del MSPI, para este fin, se utilizará el Instrumento de identificación de la línea base de seguridad actualizada para cumplir la versión 2022 de la ISO 27001. El avance en ciclo PHVA del sistema debe aumentar en 10 puntos frente al diagnóstico actual, para lograr un avance del 85%

Adicionalmente, el Oficial de Seguridad de la Información, medirá el cumplimiento del presente Plan, a través del resultado del siguiente indicador, para el cual la meta es 100%:

Cumplimiento en la implementación del Plan de Seguridad:

$$\frac{\text{Actividades del plan Ejecutadas}}{\text{Total, de Actividades programadas en el Plan}} * 100$$

10. ANEXOS

ANEXO 1. ESTRATEGIA DE SEGURIDAD DIGITAL

1. INTRODUCCIÓN

El concepto de seguridad digital como "la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio) que es la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales derivada de la realización de los fines esenciales del Estado, mediante:[1]

- La gestión del riesgo de seguridad digital.
- La implementación efectiva de medidas de ciberseguridad
- El uso efectivo de las capacidades de ciber defensa.

Durante el 2024, Colombia se ha enfrentado a desafíos considerables en seguridad, siendo el país más afectado en América Latina, con un **17%** de los ataques registrados en la región.

Esto Destaca la necesidad Urgente de Fortalecer las defensas digitales ante las amenazas emergentes:

Principales Amenazas:

Aplicaciones Publicas: Son el principal vector de ataque en Colombia, destacando la importancia de adoptar practicas seguras al usar software de terceros, con un 45% de presencia frecuentes como foco de ataque.

Ransomware: Se ha observado un aumento alarmante en este tipo de ataques, con graves repercusiones monetarias a través de la encriptación para organizaciones afectadas. Con un porcentaje de 35% es el segundo foco de ataque más representativo en Colombia, por anterior el Ministerio de Relaciones Exteriores participo en

[1] (Aprende, s.f.)

la IV Reunión Anual[2] de la iniciativa contra el Ransomware entre el 30 septiembre y el 3 octubre de 2024 en Washington DC.
Donde se reafirmó el compromiso de enfrentar conjuntamente el ransomware y fortalecer los esfuerzos conjuntos con las instituciones como la policía nacional y cibercriminal de AMERIPOL.

Filtración de Datos a través de Correo: las filtraciones de datos se produjeron mediante ataques de correo/phishing, resaltando la necesidad de concienciar sobre ciberseguridad entre los empleados, con un porcentaje de 45% de ocupación usada por los atacantes.
El Ministerio de Relaciones Exteriores se han planteado ejercicios controlados con herramientas que posee el Ministerio, para generar conciencia digital en los funcionarios.

Phishing: Los ciber delincuentes continúan usando esta táctica, buscando obtener información confidencial de usuarios a través de correos electrónicos y sitios web falsos, con un porcentaje de 22% de ocupación usada por los atacantes.

Accesos no Autorizados a Servidores y Nubes: Un aumento significativo en estas intrusiones pone en riesgo la integridad y confidencialidad de la información almacenada, con un porcentaje de 23% de ocupación usada por los atacantes.
Por esta razón es primordial adoptar modelos, estándares y marcos de trabajo en materia de seguridad digital que permitan entender, clasificar y priorizar la madurez en seguridad digital de la Ministerio de relaciones Exteriores, con esto se podrán implementar un conjunto de actividades y/o controles que aporten a la confianza digital de los activos presentes en el ciberespacio donde la comunidad esa presente e interactúa día a día.

Es así, como la Estrategia de Seguridad Digital 2025 adoptará el estándar NIST SP 800-53, el cual es un marco de trabajo publicada por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos que proporciona un conjunto completo de controles de seguridad y recomendaciones para ayudar a las organizaciones a gestionar y mejorar la seguridad de la información en sus sistemas y procesos.

En este sentido, la Dirección de Gestión de la Información y Tecnología es la encargada de realizar esta implementación, que incluye los controles tecnológicos de seguridad necesarios para el cierre de la brecha y realiza la sensibilización en temas de seguridad digita, los cuales se encuentran incluidos en el plan de sensibilización en Seguridad de la Información.

[2] (Cancilleria.gov.co, 2024)

2. OBJETIVO

Establecer medidas para desarrollar la confianza digital a través de la implementación de un conjunto de actividades priorizadas que conforman la Estrategia de Seguridad Digital del Ministerio de Relaciones Exteriores y su Fondo Rotatorio, que permite:

- Identificar mediante una metodología de seguridad digital los riesgos que debe afrontar la Ministerio de Relaciones Exteriores y su Fondo Rotatorio.
- Promover la cultura, conciencia y sensibilización en seguridad digital, mediante la formulación de un plan de sensibilización de seguridad de la información, en el cual se incluyen todos los temas relacionados con ciberseguridad
- Implementar y priorizar los controles de seguridad digital para mitigar los riesgos detectados, luego del diagnóstico realizado.
- Fortalecer las tecnologías de la información y las comunicaciones que utiliza Ministerio de Relaciones Exteriores, mediante la identificación de la necesidad de tecnologías emergentes y apropiadas que demandan los potenciales ataques del ciberespacio hoy día.
- Apoyar al modelo de seguridad y privacidad de la información en lo referente a los controles técnicos definidos y ciberseguridad.

3. ALCANCE

La presente Estrategia se conforma en un primer momento por los resultados de un diagnóstico de madurez en ciberseguridad realizado en la sede central para la vigencia 2024, sigue con en análisis de los resultados en nivel de cumplimiento y finaliza con las actividades por Función que fortalecerán la seguridad digital y la ciberseguridad y el objetivo deseado en la vigencia 2025 al 2026.

4. RESPONSABLES

La Dirección de Gestión de Información y Tecnología es la encargada de realizar la implementación de la presente estrategia la cual incluye los controles tecnológicos de seguridad necesarios para el cierre de la brecha y realiza la sensibilización en temas de seguridad Digital.

5. DEFINICIONES

Amenaza: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre

los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

Análisis de riesgos: Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de estas, a fin de determinar los controles adecuados para tratar el riesgo.

Análisis de vulnerabilidades: Consiste en la búsqueda y documentación de fallos, carencias o debilidades físicas (inundaciones, incendios, controles de acceso…) y lógicas (configuraciones, actualizaciones...) en un sistema informático, que puedan ser empleados por terceros con fines ilícitos, suponiendo un riesgo para la organización y los propios sistemas. El análisis propone vías de mitigación a implementar para subsanar las deficiencias encontradas y evitar ataques a los sistemas informáticos.

Aseguramiento: Proceso que trata de reducir las vulnerabilidades y agujeros de seguridad presentes en un sistema, creando un entorno lo más seguro posible siguiendo los principios de: mínima superficie de exposición, mínimos privilegios y defensa en profundidad. Entre las acciones que se realizan para alcanzar este propósito destacan la eliminación de recursos, servicios o programas que no se utilizan, baja de usuarios o cambio de las credenciales o configuraciones establecidas por defecto.

Ciberataque: Intento deliberado de un ciber delincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema

Control de acceso: Sistema de verificación que permite el acceso a un determinado recurso si la persona o entidad tiene los derechos necesarios para solicitarlo. Este acceso puede ser a recursos de tipo físico (por ejemplo, a un edificio o un departamento) o lógicos (por ejemplo, a un sistema o una aplicación software específica).

Copia de seguridad (backup): Proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperar los datos contenidos en caso de fallo del primer soporte de alojamiento.

CSIRT: Acrónimo de *Computer Security Incident Response Team*, también conocido en español como equipo de respuesta a incidentes de seguridad informáticos, es el equipo encargado de recibir, comprobar y responder a incidentes que se detecten en su área de actuación. Es considerado como el equivalente en Europa de su contraparte estadounidense CERT.

Detección de incidentes: Sistema que analiza determinados parámetros y elementos que sirven para monitorizar, detectar y verificar indicios de posibles incidentes de seguridad, que pueden registrarse en el sistema objeto de estudio y evaluación.

Escaneo de vulnerabilidades: Actividad en la que se buscan vulnerabilidades en redes y sistemas, mediante diferentes técnicas y aplicaciones especializadas, con el fin de identificarlas y subsanarlas para evitar que sean utilizadas por los ciberdelincuentes en su beneficio. El escaneo se centra en las aplicaciones, puertos y servicios desplegados en una empresa.

Gestión de incidentes: Listado de procedimientos previamente documentados sobre los pasos a seguir en caso de detectar una amenaza de ciberseguridad en la empresa. La gestión de incidentes está orientada a mitigar en el menor tiempo posible un incidente de seguridad identificándolo y asignando el personal que dará respuesta al mismo dentro de unos parámetros predefinidos.

Impacto: Medida del efecto que produce un incidente, desastre, problema o cambio en los niveles de servicio de una empresa y cómo se ven afectados en el caso de que se materialice dicha amenaza.

Incidente de seguridad: Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

Intrusión: Acción provocada por un atacante o usuario malintencionado, que se aprovecha de una vulnerabilidad en el sistema para conseguir acceder a un área o dispositivo sin autorización con el objetivo de realizar actividades ilegítimas.

Múltiple factor de autenticación (MFA): Esquema de autenticación básica a la que se añade otro factor como puede ser un código enviado a un móvil, huella dactilar, sistema OTP, etc., más seguro que la autenticación simple.

Política de seguridad: Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos. Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información.

Respuesta de incidentes: Se trata de un plan o guía con el que poder dar respuesta a posibles incidentes de ciberseguridad en la empresa. Dicha guía debe contemplar varios puntos esenciales, detección y registro del incidente, análisis y evaluación, notificación y equipo o personal encargado de su resolución, así como

soluciones y mejoras para evitar futuras incidencias. Todo ello siempre atendiendo a la ley RGPD en materia de protección de datos.

Riesgo: Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo pueda ser elevado.

SOC: Del inglés *Security Operations Center*; en español, centro de operaciones en seguridad. Se trata de un equipo cualificado específicamente en ciberseguridad con las herramientas necesarias para poder analizar, investigar y dar soporte convenientemente a posibles eventos de ciberseguridad corporativos. Un SOC puede ser externo o interno, y su objetivo es evitar y mitigar posibles ataques en la empresa, constituyendo lo que podríamos llamar contramedidas ante un ciberataque.

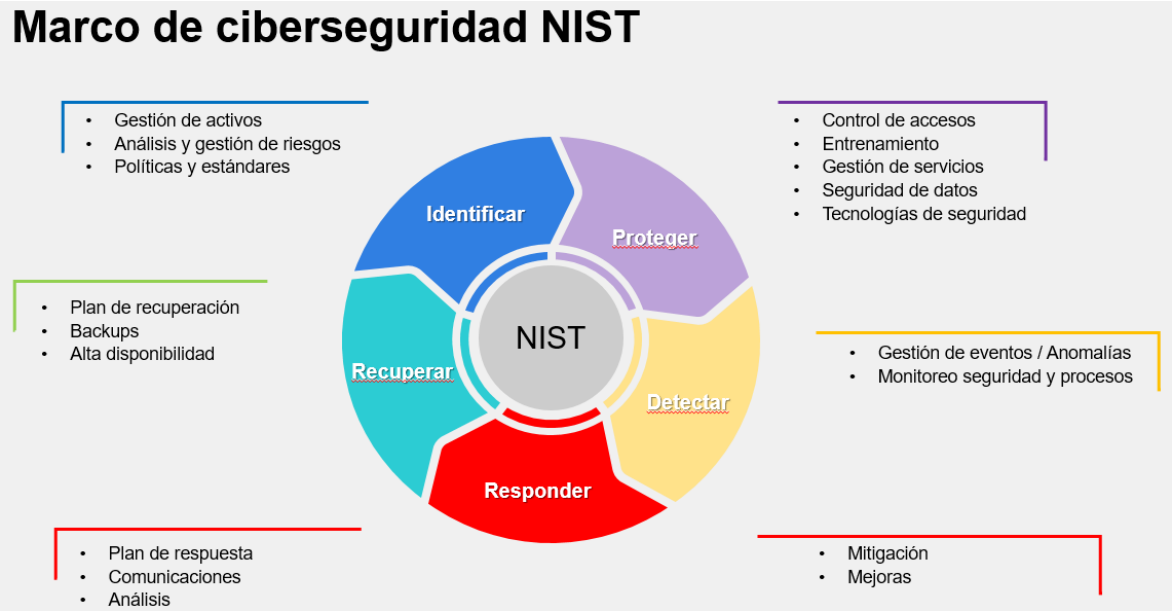
Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto.

6. DIAGNOSTICO

Durante el segundo semestre de 2024 se realizó un diagnóstico de madurez en seguridad digital y ciberseguridad bajo el marco de trabajo en ciberseguridad de la NIST SP 800-53, evaluado por un fabricante líder en soluciones y servicios de ciberseguridad.

El ejercicio consistió en una dinámica de preguntas y respuestas, en donde el evaluador iba abarcando las funciones del estándar (Identificar, Proteger, Detectar, Responder, Recuperar) para luego clasificar el nivel madurez evaluado (Inexistente, Inicial, Definido y optimizado).

Nivel de madurez: Cuando se habla de un nivel de madurez se debe entender como un conjunto de prácticas, preestablecidas por el modelo, que se deben garantizar en su conjunto



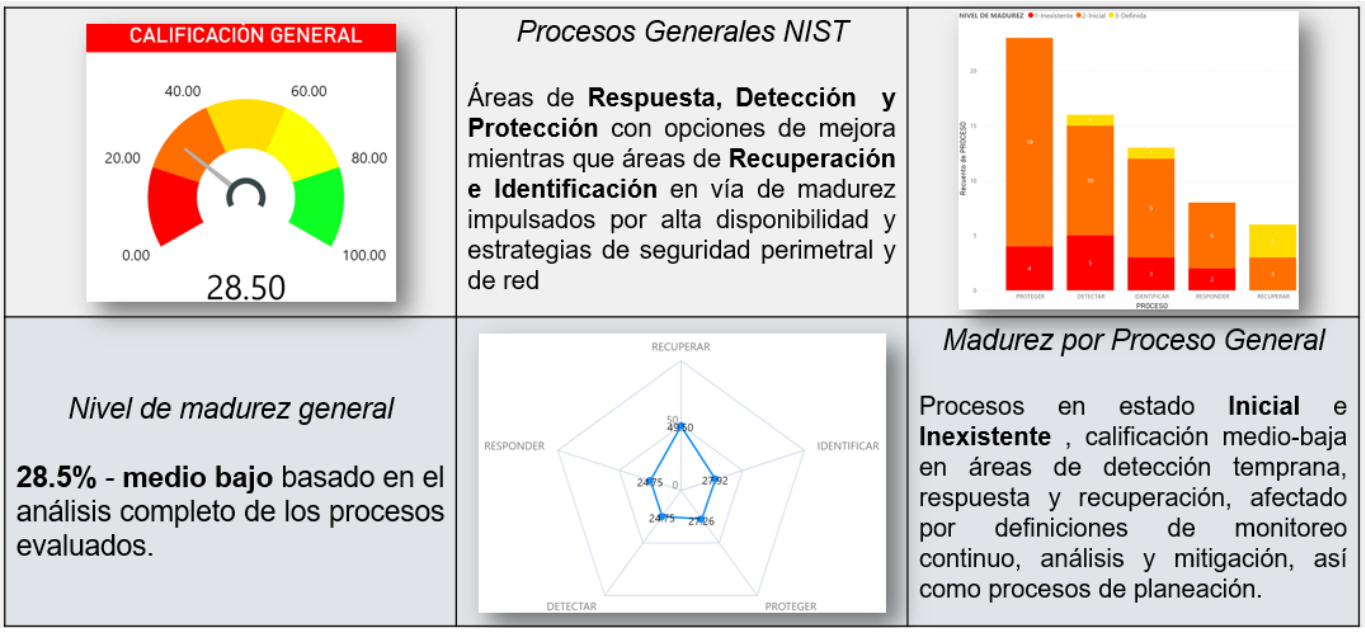
Gráfica 1 - Arquitectura del marco de trabajo de ciberseguridad del NIST (CSF)

Ponderación	% de Cumplimiento	Criterio Explicación	Explicación
0	0%	1- INEXISTENTE	Falta total de un proceso reconocible. La organización ni siquiera ha reconocido que hay un problema que resolver.
1	33%	2-INCIAL	Este proceso es manual y tiene un cubrimiento muy básico
2	66%	3-DEFINIDO	Este proceso esta Automatizado por medio de una herramienta tecnológica y tiene un cubrimiento parcial
3	100%	4- OPTIMIZADO	Este proceso esta Automatizado por medio de una herramienta tecnológica, tiene un cubrimiento TOTAL y cuenta con un ciclo PHVA de mejora continua

Fuente: https://es.linkedin.com/pulse/implementando-el-cybersecurity-framework-del-nist-g%C3%B3mez-morales

6.1 RESULTADOS GENERALES DEL DIAGNÓSTICO

Como resultado general, en la sumatoria de los dominios evaluados (identificar, proteger, detectar, responder y recuperar), se Obtuvo un puntaje 28.5%, Esto indica que el Ministerio de Relaciones Exteriores y su Fondo Rotatorio debe Implementar acciones para mejorar su postura de seguridad en cada control evaluado.

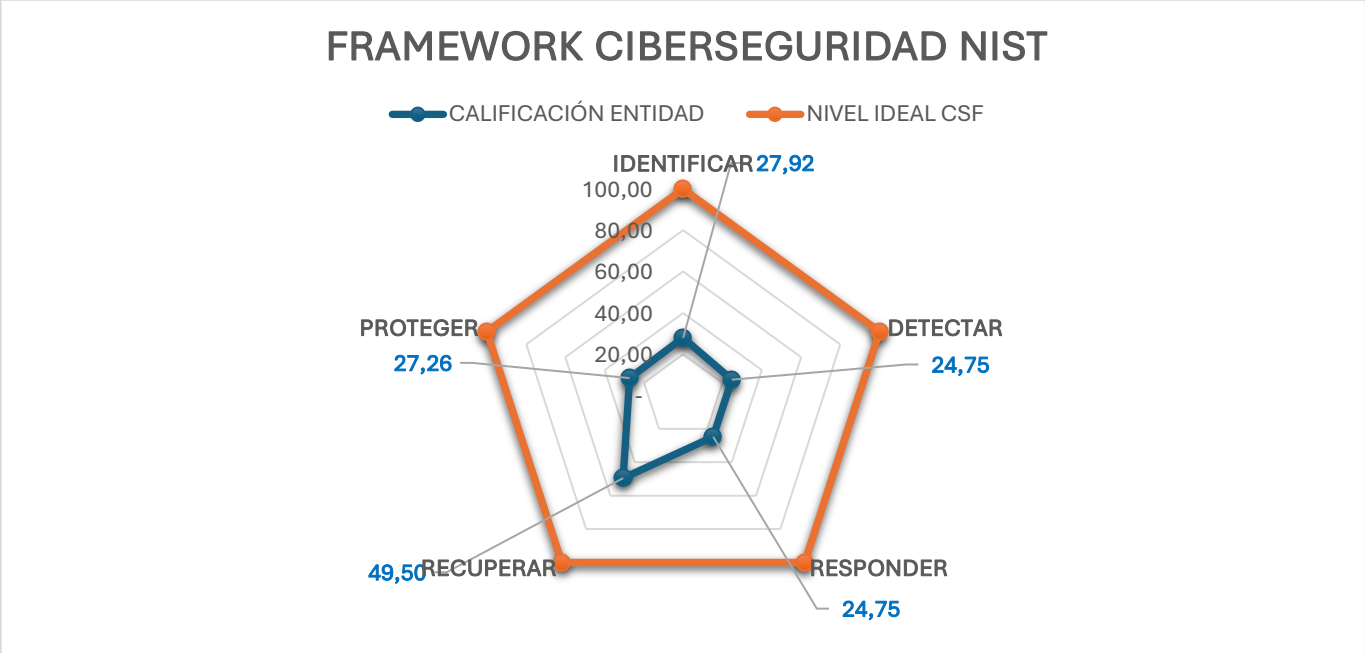


Gráfica 2- Evaluación de ciberseguridad – Estado General

6.2 METODOLOGÍA PARA LA ESTRATEGIA

Se adoptarán las cinco funciones del Marco de Trabajo de Ciberseguridad de la NIST, relacionando cada una de ellas (identificar, proteger, detectar, responder, recuperar) con los controles definidos como dominios técnicos por el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual servirá de soporte al habilitador transversal de la seguridad de la información política de Gobierno Digital.

De acuerdo con el autodiagnóstico NIST realizado, en cada función evaluada se identificaron procesos en distintos niveles de madurez: procesos inexistentes, procesos iniciales, procesos definidos y procesos optimizados.



Grafica No.1. Calificación Framework de Ciberseguridad NIST

La presente estrategia se enfocará en desarrollar actividades, crear procedimientos y establecer controles que permitan que los calificados como inexistentes e iniciales evolucionen hacia procesos definidos. Para los ya definidos, se establecerán actividades orientadas al monitoreo y la automatización, mientras que, para los optimizados, se diseñarán acciones dirigidas al mejoramiento continuo.

Categoría NIST	Procesos	Recomendaciones
Identificar	*Fuentes de Inteligencia de Amenazas de Terceros para alimentar los sistemas de Ciberseguridad.	Implementar un SOAR con las herramientas existentes como el EDR y AV para generar casos de uso y escalamientos de Riesgo a las Áreas encargadas
	*Proceso de Gestión de Riesgos cibernéticos debe adelantarse mediante la implementación de soluciones para la correlación de eventos y vulnerabilidades y su posterior análisis basados en los riesgos de ciberseguridad	Implementar un sistema robusto que se integre a herramientas (SIEM y Vulnerabilidades) y que reporte en tiempo real amenazas presentes para reducir el riesgo

Categoría NIST	Procesos	Recomendaciones
	*Auditoria o Evaluación de Terceros en términos de Ciberseguridad	Mantener en las renovaciones de los contratos los servicios de ciberseguridad con proveedores y aliados, debe tener ANS o SLA en los contratos alinear los procesos del servicio de ciberseguridad con las políticas de seguridad de la información del Ministerio
Proteger	Acceso lógico a los activos tecnológicos es protegido con herramientas de AAA centralizadas, MFA y métodos de inspección de comportamiento	Extender la Doble Autenticación al inicio de sesión de servidores críticos mediante la herramienta de Microsoft, confirmar el uso de servidores de TACACS+ y RADIUS en equipos Activos (Sw,Router,FW,Waf). A nivel de autenticación de Redes implementar Network Access Control - NAC
	Los usuarios, dispositivos y otros activos están autenticados con múltiples factores de autenticación en VPNs y aplicaciones criticas	Garantizar la implementación de la herramienta de autenticación de Microsoft en las VPNs y servidores
	Los datos en reposo están protegidos en cuanto a confidencialidad e integridad de la información (monitoreo automático)	Implementación de DLP en fuentes donde se puede presentar fugas de información (Correo, Chat, meeting)
	Se cuentan con líneas base de sistemas operativos y aplicaciones incorporando principios de ciberseguridad.	Validar usuario con excesos de privilegios, usar jerarquías y custodia de usuarios genéricos, mantener la política de instalación de software permitido, utilizar software de endurecimiento como Microsoft Security Compliance Toolkit o nessus
Detectar	Monitoreo de seguridad, que permita centralizar la información de detección de amenazas de los principales sistemas de la organización	Implementar un SIEM con un proveedor mediante un servicio de monitoreo que permita realizara casos de usos y escalamiento de la gestión
	Los eventos de seguridad se retienen y almacenan por un tiempo establecido, que permita realizar tareas de investigación	Implementar el almacenamiento de logs tanto de soluciones on premise como cloud con una retención mínima de 6 meses para soluciones (FW, SERVIDORES, WAF) o aplicaciones críticas para el Ministerio
	Monitoreo de la actividad del proveedor de servicios externo para detectar posibles eventos de ciberseguridad	Implementar el servicio de monitoreo 7x24 que permita una identificación temprana y seguimiento de posibles eventos o incidentes de seguridad.

Categoría NIST	Procesos	Recomendaciones
	Funciones y responsabilidades de gestión de incidentes están definidas con lo que se garantiza la responsabilidad de las áreas de tecnología y otras áreas en los procesos de manejos de anomalías	Se debe alinear el procedimiento de Incidentes con sus respectivas fases y matriz de escalamiento para garantizar tanto con los aliados tecnológicos como áreas idóneas para la gestión temprana y oportuna del incidente.
	Monitoreo de infraestructura en nube privada y/o publica que permita identificar amenazas, infecciones y comportamientos maliciosos	Implementar con un tercero o proveedor un monitoreo tanto de performance como seguridad que permita tener una visión global de los recursos vitales de la institución para así prevenir y actuar en una medida de tiempo oportuna algún evento que puede afectar la continuidad de negocio
Responder	Proceso de Análisis Forense a los incidentes de Ciberseguridad	Con el proceso de almacenamiento de log y eventos se puede realizar el análisis forense de los incidentes de seguridad; se debe tener presente que los servidores deben disponer activo el almacenamiento de evento enviado al syslog, también permitir el XDR instalado para validar comportamientos y poder implementar Sandbox para análisis de malware.
	Componentes que integran la arquitectura de seguridad si interconectan entre sí, para reaccionar automáticamente ante una amenaza identificada en alguno de ellos	Implementar soluciones de SOAR que permita orquestar lo componentes activos de Red(FW,WAF,XDR,AV) con casos de uso aplicados según casos de uso generados con el tercero contratado
Recuperar	Actualizar las estrategias de recuperación y la base de datos de lecciones aprendidas	Alinear la gobernanza con ejercicios de DRP (Recuperación de Desastres), validar que los Backups de aplicaciones críticas o servidores este activo y replicando
	Mejora y pruebas continuas de los mecanismos y procedimientos de recuperación	Generar pruebas de DRP por lo menos 2 veces por año de manera semestral para verificar sistema de redundancia y replicaciones
	Generan comunicaciones post incidentes tanto externa como internamente	Alinear los informes ejecutivos de evento a la Dirección de tecnológica en caso de presentarse algún incidente donde mediante mesas de trabajo previas se puedan gestionar con las áreas involucradas

Las actividades necesarias para mejorar la postura de seguridad digital y ciberseguridad para la Vigencia 2025 se encuentran documentadas en el Numeral 7. Cronograma y Entregables del Presente Plan.