



Gobierno del
Cambio



COLOMBIA
POTENCIA DE LA
VIDA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2026

En la Superintendencia de Sociedades trabajamos para promover
empresas innovadoras, productivas y sostenibles.

www.supersociedades.gov.co

webmaster@supersociedades.gov.co

Línea única de atención al ciudadano: 01-8000 - 11 43 10

Tel Bogotá: (601) 2201000
Colombia





Tabla de Contenido

INTRODUCCIÓN	4	
1. OBJETIVO	4	
1.1. OBJETIVO GENERAL		4
1.2. OBJETIVOS ESPECIFICOS		5
2. ALCANCE	5	
3. MARCO NORMATIVO	5	
4. RESPONSABILIDADES	10	
5. DEFINICIONES	10	
6. DESARROLLO DEL PLAN	12	
6.1. OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN(SGSI)		13
6.1.1. Política de seguridad de la información.	13	
6.1.2. Objetivos de Seguridad de la información	13	
6.1.3. Diagnóstico del Sistema de Seguridad y Privacidad de la Información	14	
6.2. IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (Estrategia de planificación y control operacional)		18
6.3. MATRIZ DE ESTRATEGIA DE PLANIFICACIÓN Y CONTROL OPERACIONAL	20	
6.3.1. DOMINIO IDENTIFICAR		27
6.3.2. DOMINIO PROTEGER		28
6.3.3. DOMINIO DETECTAR		28
6.3.4. DOMINIO RESPONDER		29
6.3.5. DOMINIO RECUPERAR		29
7. RECURSOS	34	
8. SEGUIMIENTO Y MEDICIÓN	34	
8.1. INDICADORES		34

En la Superintendencia de Sociedades trabajamos para promover
empresas innovadoras, productivas y sostenibles.

www.supersociedades.gov.co

webmaster@supersociedades.gov.co

Línea única de atención al ciudadano: 01-8000 - 11 43 10

Tel Bogotá: (601) 2201000

Colombia



TR- CO177851

TR- CO177853

TR- CO177858

CS - CCR279481

CO - 071 / 2021 / ICONTEC



CONTROL DE CAMBIOS

Tabla 1. Cuadro de control			
Versión	Fecha	Instancia de Aprobación	Descripción
01	16-dic-2022	Comité Institucional de Gestión y Desempeño	Formulación General del Plan estratégico de Tecnologías de la Información PETI 2023-2026.
02	05-Jul-2023	Comité Institucional de Gestión y Desempeño	Se realiza ajuste de acuerdo con el Diagnóstico realizado y las estrategias del Plan Nacional de Desarrollo

MARCO ESTRATEGICO

ARTICULACION MARCO ESTRATEGICO	
ODS	Objetivo 16. Paz, Justicia e instituciones sólidas
PND - 2022 - 2026	Seguridad Humana y Justicia Social
PES - 2023-2026	Objetivo No.6 : Transformación Institucional: Transformar la capacidad y la respuesta institucional para el fortalecimiento de la confianza y la participación ciudadana en las entidades del Sector
PEI - 2023-2026	Objetivo No.3 Aumentar la excelencia en el servicio a través del fortalecimiento de la oferta de valor a los usuarios de manera efectiva y pronta.
POLITICA MIPG	Política de Gobierno Digital Política de Seguridad Digital



INTRODUCCIÓN

La Superintendencia de Sociedades, para el desarrollo de sus fines misionales, así como para la ejecución de sus procesos, trámites y servicios, cuenta con una infraestructura tecnológica que está compuesta por Hardware, Software, Comunicaciones, Bases de datos, instalaciones físicas, hiperconvergencia, servicios en la nube, seguridad perimetral, sistemas de control de acceso y otros elementos auxiliares, que permiten una alta disponibilidad, integridad, confidencialidad y seguridad de la información tanto pública como privada; todo, dentro del marco de la Arquitectura Empresarial (AE), la transformación digital y el uso de tecnologías emergentes como la Inteligencia Artificial y Big Data, impulsados por el Gobierno Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), los planes intersectoriales y los planes de implementación de Gobierno Digital (Decreto 1008 de 2018), Seguridad Digital (Resolución Número 00500 de marzo 10 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”), el modelo de Seguridad y Privacidad de la Información, los cuales se están implementado de manera rigurosa y formal en la Superintendencia de Sociedades.

Dentro de este marco normativo y acorde con la arquitectura empresarial implementada, la Superintendencia de Sociedades ha adoptado un Sistema de Gestión Integrado (SGI) que comprende las normas (NTC ISO 9001 Gestión de Calidad, NTC ISO/IEC 27001 Sistema de Gestión de la Seguridad de la Información, NTC ISO 14001 sistema de Gestión Ambiental, El Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), NTC 5906 (Centro de Conciliación y Arbitraje), el Modelo Estándar de Control Interno –MECI- y el Modelo Integrado de Planeación y Gestión definido en el Decreto 1499 de 2017.).

La implementación del Sistema de Gestión de Seguridad de la Información (ISO27001:2013) desde el año 2011 ha servido como soporte del cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), debido a que esta norma es el fundamento del MSPI. Con esto se ha logrado un alto cumplimiento de este modelo que soporta a su vez la seguridad y privacidad de la Información como habilitador transversal de la Política de Gobierno Digital.

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

1. OBJETIVO

1.1. OBJETIVO GENERAL

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y la continuidad del servicio, para fortalecer los procesos, los trámites y los servicios de la

En la Superintendencia de Sociedades trabajamos para promover empresas innovadoras, productivas y sostenibles.

www.supersociedades.gov.co

webmaster@supersociedades.gov.co

Línea única de atención al ciudadano: 01-8000 - 11 43 10

Tel Bogotá: (601) 2201000

Colombia



TR- CO177851

TR- CO177853

TR- CO177858

CS - CE279481

CO - 071 / 2021 / ICONTEC



Superintendencia de Sociedades, garantizando la disponibilidad, confidencialidad e integridad de sus activos de información.

1.2. OBJETIVOS ESPECIFICOS

- Implementar la protección de los activos de información de la Superintendencia de Sociedades, con base en los criterios de confidencialidad, integridad y disponibilidad.
- Sensibilizar a los servidores públicos y contratistas de la Superintendencia de Sociedades acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la Entidad.
- Evaluar el cumplimiento de los requisitos y controles de seguridad de la información para fortalecer los procesos, trámites y servicios de la Superintendencia de Sociedades.
- Monitorear el cumplimiento de requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico y alertamiento.
- Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información.

2. ALCANCE

El Plan de Seguridad y Privacidad de la información identifica e incluye las actividades para:

- Continuar con el cumplimiento y certificación de la norma ISO27001:2013 o versión vigente para todos los procesos de la Superintendencia de Sociedades.
- Aplicar la gestión del ciclo (PHVA) de operación del modelo de seguridad y privacidad de la información (MSPI).
- Asegurar la disponibilidad, confidencialidad e integridad de los activos de información de la Superintendencia de Sociedades.

3. MARCO NORMATIVO

JERARQUÍA	NUMERO / FECHA	TITULO
Ley	527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones
Ley	1273 del 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones

En la Superintendencia de Sociedades trabajamos para promover empresas innovadoras, productivas y sostenibles.

www.supersociedades.gov.co

webmaster@supersociedades.gov.co

Línea única de atención al ciudadano: 01-8000 - 11 43 10

Tel Bogotá: (601) 2201000

Colombia





JERARQUÍA	NUMERO / FECHA	TITULO
Ley	1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley	2108 de 2021	Ley de internet como servicio público esencial y universal" opor medio de la cual se modifica la ley 1341 de 2009 y se dictan otras disposiciones
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	1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto	886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Decreto	2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
Decreto	1083 de 2015	Artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos y publicarlos, en su respectiva página web, a más tardar el 31 de enero de cada año. (Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Plan de Seguridad y Privacidad de la Información, entre otros).
Decreto	1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto	728 de 2017	Se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del decreto único reglamentario del sector TIC, 1078 de 2015, "Implementación de zonas de acceso público a internet inalámbrico en entidades públicas del orden nacional para el fortalecimiento del modelo de gobierno digital.
Decreto	1499 de 2017	El Departamento Administrativo de la Función Pública, reglamentó el Sistema Integrado de Planeación y Gestión y actualizó el modelo para su implementación, denominado "Modelo Integrado de Planeación y Gestión – MIPG"
Decreto	1008 de 2018	Por medio del cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del

En la Superintendencia de Sociedades trabajamos para promover empresas innovadoras, productivas y sostenibles.

www.supersociedades.gov.co

webmaster@supersociedades.gov.co

Línea única de atención al ciudadano: 01-8000 - 11 43 10

Tel Bogotá: (601) 2201000

Colombia



CO - 071 / 2021 / ICONTEC



JERARQUÍA	NUMERO / FECHA	TITULO
		sector de Tecnologías de la Información y las Comunicaciones.
Decreto	1389 de 2022	Por el cual se adiciona el Título 24 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para la gobernanza en la infraestructura de datos y se crea el Modelo de gobernanza de la infraestructura de datos
Resolución	511-004571 de Agosto de 2012	Por la cual se delegan funciones y asignan competencias
Resolución	511-004064 de Julio de 2012	La cual crea los grupos internos de trabajo que conforman la Superintendencia de Sociedades .
Resolución	165-2748 de 2005	Por la cual son asignadas funciones para el manejo y control del Sistema de Gestión de la Superintendencia de Sociedades
Resolución	3564 de 2015	Reglamentaciones asociadas a la ley de Transparencia y acceso a la información pública
Resolución	510-000356 de 2015	Por medio de la cual se implementa el Plan Piloto de Teletrabajo en la Superintendencia de Sociedades
Resolución	165-000368 de 2018	Por medio de la cual se adopta la política de Gestión Integral para la gestión socialmente responsable y designa el Representante de la Alta Dirección para el Sistema de Gestión Integrado.
Resolución	100-003113 del 05/03/2019	Por medio de la cual se asignan unas funciones y se definen los Grupos internos de trabajo en la Superintendencia de Sociedades.
Resolución	100-000040 de 2021	Por medio de la cual se asignan unas funciones y se definen los grupos internos de trabajo en la Superintendencia de Sociedades
Resolución MINTIC	1519 de 2000	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Resolución MINTIC	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.

En la Superintendencia de Sociedades trabajamos para promover empresas innovadoras, productivas y sostenibles.

www.supersociedades.gov.co

webmaster@supersociedades.gov.co

Línea única de atención al ciudadano: 01-8000 - 11 43 10

Tel Bogotá: (601) 2201000

Colombia



CO - 071 / 2021 / ICONTEC



JERARQUÍA	NUMERO / FECHA	TITULO
Resolución MINTIC	746 de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021.
Directiva Presidencial	02 de 2002	Derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software)
Directiva Presidencial	03 de marzo de 2021	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
Directiva Presidencial	24 de febrero de 2022	Reiteración de la política pública en materia de seguridad digital.
Documento	CONPES 3650 de 2010	El presente documento somete a consideración del Consejo Nacional de Política Económica y Social – Conpes, la declaratoria del Programa Agenda de Conectividad - Estrategia de Gobierno en Línea que el Ministerio de Tecnologías de la Información y las Comunicaciones ha venido desarrollando a través del proyecto de inversión “Implementación y Desarrollo Agenda de Conectividad”, como de importancia estratégica para continuar con su implementación y promoción en el orden nacional y territorial.
Documento	CONPES 3701 de 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa
Documento	CONPES 3854 de 2016	Política Nacional de Seguridad Digital
Documento	NTC 5854 de 2012	Accesibilidad de páginas web
Circular	52 de 2007	Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.
Circular Interna	05 de 2000	Uso de software pirata
Circular Interna	25 de 2000	Agenda de conectividad del gobierno colombiano

En la Superintendencia de Sociedades trabajamos para promover empresas innovadoras, productivas y sostenibles.

www.supersociedades.gov.co

webmaster@supersociedades.gov.co

Línea única de atención al ciudadano: 01-8000 - 11 43 10

Tel Bogotá: (601) 2201000

Colombia



TR- CO177851

TR- CO177853

TR- CO177858

CS - CER279491

CO - 071 / 2021 / ICONTEC



JERARQUÍA	NUMERO / FECHA	TITULO
Circular Interna	07 de 2001	Reglamento sobre el uso del correo electrónico y el servicio de Internet
Circular Interna	11 de 2001	Implantación del Sistema de Gestión
Circular Interna	03 de 2004	Implantación de los módulos de seguridad y notificaciones del Sistema de Gestión.
Norma técnica colombiana	NTC/ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.
Norma técnica colombiana	NTC/ISO 27001:2013	Gestión del Riesgo. Principios y directrices.
Documento Técnico Externo	2016	Modelo de Seguridad y Privacidad de la Información – MSPI Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Versión 3.0.2, julio de 2016
Documento Técnico Externo	2019	Manual para la Implementación de la Política de Gobierno Digital Implementación de la Política de Gobierno Digital (Decreto 1008 de 2018). Versión 7, abril de 2019.
Documento del Sistema de Gestión Integral	GC-I-001	Instructivo para la identificación, clasificación, valoración y etiquetado de activos de información.
Documento del Sistema de Gestión Integral	GC-I-002	Instructivo para la gestión de riesgos de seguridad de la información.

En la Superintendencia de Sociedades trabajamos para promover empresas innovadoras, productivas y sostenibles.

www.supersociedades.gov.co

webmaster@supersociedades.gov.co

Línea única de atención al ciudadano: 01-8000 - 11 43 10

Tel Bogotá: (601) 2201000

Colombia



TR- CO177851

TR- CO177853

TR- CO177858

CS - CER279491

CO - 071 / 2021 / ICONTEC



4. RESPONSABILIDADES

De acuerdo con el documento GC-MO-001 Modelos del sistema de Gestión Integrado, numeral 2.1 MODELO DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, se define el gobierno de seguridad de la información, el cual se encuentra conformado por los roles de Oficial de Seguridad de la Información, Administrador de Seguridad Informática – Grupo de Seguridad e Informática Forense, Dueños de los procesos, Administrador de Seguridad Física, Control Interno y Oficial de Protección de Datos, quienes tienen unas responsabilidades específicas a cada rol.

5. DEFINICIONES

- **Activo de Información:** Es todo aquello que posee valor para una entidad, como: elementos de hardware, software de procesamiento, almacenamiento y comunicaciones, bases de datos, información física y digital, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa, administrativa de la entidad, entre otros.
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
- **Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a la organización.
- **Análisis del riesgo:** Proceso sistemático para entender la naturaleza del riesgo y deducir su nivel.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Custodio del activo de información:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. (tomado de la “Guía para la gestión y clasificación de activos de información”).



Gobierno del Cambio

- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. (tomado de la “Guía para la gestión y clasificación de activos de información”).
- **Contratistas:** Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. (tomado de la “Guía para la gestión y clasificación de activos de información”).
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Guía:** documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Información:** Es un activo impreso, escrito, físico, digital, electrónico que se crea, procesa, envía y transfiere por los procesos.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos. (tomado de la “Guía para la gestión y clasificación de activos de información”).
- **Inventario de activos de Información:** Identificación de todos aquellos recursos que posean valor para la entidad (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) contemplados dentro del alcance del SGSI, los cuales requieran ser protegidos de potenciales riesgos.
- **Mapa de Riesgos:** Documento con la información resultante de la gestión del riesgo.
- **Norma:** Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.
- **Oficial de Seguridad de la Información:** Profesional responsable de alinear las iniciativas de seguridad de la información con los objetivos misionales, garantizando que los bienes y las tecnologías de la información están adecuadamente protegidos.
- **Partes Involucradas (Stakeholders):** personas y organizaciones que pueden ser afectadas, son afectadas por, o perciben que ellos mismos pueden ser afectados por una decisión o actividad.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Política de riesgos:** Orientación general en torno a la administración de riesgos emanada de la Ala Dirección. Política de riesgos: orientación general en torno a la administración de riesgos emanada de la Ala Dirección.
- **Probabilidad:** Posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de frecuencia o factibilidad.
- **Propietario del activo de información:** Persona, grupo interno de trabajo o una dependencia al que se ha dado la responsabilidad formal por la seguridad de un activo o

En la Superintendencia de Sociedades trabajamos para promover
empresas innovadoras, productivas y sostenibles.

www.supersociedades.gov.co

webmaster@supersociedades.gov.co

Línea única de atención al ciudadano: 01-8000 - 11 43 10

Tel Bogotá: (601) 2201000

Colombia



TR- CO177851

TR- CO177853

TR- CO177858

CS - CER279481

CO - 071 / 2021 / ICONTEC



una categoría de activos de información. No significa que el activo pertenece al dueño en un sentido legal. Los propietarios de activos de información son responsables de manera formal por garantizar que los mismos, estén seguros mientras están siendo desarrollados, producidos, mantenidos, utilizados y almacenados (ciclo de vida del activo de información).

- **Riesgo:** Posibilidad de que algo suceda y genere un impacto sobre los objetivos. Está medido en términos de probabilidad de ocurrencia e impacto. *Nota: El riesgo con frecuencia se especifica en términos de un evento o circunstancia y las consecuencias que pueden derivarse de este. Es medido en términos de la combinación de la probabilidad de ocurrencia y las consecuencias del mismo.*
- **Riesgo de Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información (ISO/ IEC 27000).
- **Riesgo de Seguridad Digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía, la integridad, el orden y los intereses de la entidad. Incluye aspectos relacionados con ambiente físico, digital y personas.
- **Rol:** Papel, función que alguien o algo desempeña.
- **Seguridad de la Información:** Conjunto de medidas preventivas y reactivas que permiten asegurar que los activos de información mantengan la confidencialidad, disponibilidad e integridad.
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Usuario:** Persona que hace uso, o tiene acceso al activo de información, y tiene la responsabilidad de tomar conciencia y adoptar los requisitos de seguridad de la información, definidos y establecidos para los mismos.
- **Vulnerabilidad:** Vulnerabilidad: Una debilidad de un sujeto o sistema expuesto a una amenaza, correspondiente a su predisposición intrínseca a ser afectado o ser susceptible de sufrir pérdida. En un sistema puede ser aprovechada para violar el comportamiento deseado del mismo relativo a la protección, seguridad, confiabilidad, confidencialidad, disponibilidad e integridad de la información.

6. DESARROLLO DEL PLAN

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.

Entendiendo que la Superintendencia de Sociedades está en cumplimiento de la norma ISO 27001:2013, que se encuentra certificada en dicha norma y que se encuentra en la fase de



mejora continua, es necesario que, en cada vigencia, realice el autodiagnóstico, prepare y ejecute un plan de Seguridad y Privacidad de la Información, para garantizar su continuidad.

6.1. OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN(SGSI)

6.1.1. Política de seguridad de la información.

La superintendencia de Sociedades cuenta con un modelo de gestión integrado (MGI) que tiene establecida, aprobada y publicada, una política del Sistema de Gestión Integrado, en la cual se especifican las diferentes políticas de cada sistema de gestión.

Específicamente para Seguridad de la Información, en dicho manual en el numeral 4 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. Se relacionan otras políticas que se articulan con la seguridad de la información, como son, numeral 7 POLÍTICA PARA EL GOBIERNO DE LA INFORMACIÓN, numeral 8 POLÍTICA DE LABORATORIO FORENSE, numeral 9 POLÍTICA DE GOBIERNO DIGITAL, numeral 10 POLÍTICA DE SEGURIDAD DIGITAL, numeral 11 POLITICA DE PROTECCIÓN DE DATOS PERSONALES.

Estas políticas se pueden consultar en el manual GC-PO-001 DOCUMENTO DE POLITICAS DEL SGI, en el sistema de gestión Integrado (SGI), Mapa de procesos, proceso de Gestión Integral.

La Alta Dirección mediante Resolución 165-000638 del 15 de agosto de 2018 aprobó la Política, los Objetivos y asignó el rol y dio autoridad al Jefe de la Oficina Asesora de Planeación como su representante para garantizar que el sistema de gestión es conforme con los requisitos de las normas que integran el SGI.

6.1.2. Objetivos de Seguridad de la información

En la medida que el Sistema de gestión de seguridad de la Información, se encuentra incluido dentro del Sistema de Gestión Integrado, los objetivos del SGI también integran los objetivos de Seguridad de la Información, estos son:

- Aumentar la satisfacción de los grupos de interés.
- Agilizar, simplificar y flexibilizar los procesos internos para hacer más eficientes la atención de los trámites y otros procedimientos administrativos que presta la Entidad.
- Minimizar el impacto y/o la posibilidad de ocurrencia de los riesgos e incidentes institucionales en los procesos críticos de la Entidad.
- Incrementar la cultura de seguridad de la información en los funcionarios, terceros y contratistas.
- Mejorar las competencias de los funcionarios que permitan la prestación del servicio de manera más eficiente.
- Cumplir con la legislación y los requisitos ambientales aplicables a la Entidad.
- Optimizar el consumo de los recursos naturales.

En la Superintendencia de Sociedades trabajamos para promover empresas innovadoras, productivas y sostenibles.

www.supersociedades.gov.co

webmaster@supersociedades.gov.co

Línea única de atención al ciudadano: 01-8000 - 11 43 10

Tel Bogotá: (601) 2201000

Colombia



TR- CO177851

TR- CO177853

TR- CO177858

CS - CER279481

CO - 071 / 2021 / ICONTEC



Gobierno del Cambio

- Proteger el medio ambiente a través de la implementación de los programas del Sistema de Gestión Ambiental.
- Fomentar en los funcionarios una mayor conciencia ambiental.

La seguridad de la información es un componente transversal que se aplica a todos los procesos. Sus objetivos se alinean a los objetivos integrados, pero hay 3 exclusivos que se integran como son:

- Minimizar el impacto y/o la posibilidad de ocurrencia de los riesgos e incidentes institucionales en los procesos críticos de la Entidad.
- Incrementar la cultura de seguridad de la información en los funcionarios, terceros y contratistas.
- Mejorar las competencias de los funcionarios que permitan la prestación del servicio de manera más eficiente.

6.1.3. Diagnóstico del Sistema de Seguridad y Privacidad de la Información

De acuerdo con el modelo de Seguridad y Privacidad de la Información emitido por MINTIC, y a través de las diferentes vigencias y adecuación de normatividades, la Superintendencia de Sociedades, se encuentra en la fase de mejoramiento de dicho modelo y para tal fin, realizó el diagnóstico de implementación del MSPI a través del instrumento correspondiente.

Los niveles definidos por el instrumento para realizar la medición son los siguientes:

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentran gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuentan con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Tabla No.1: Niveles de Avance según el Instrumento de Diagnóstico de MINTIC

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
 Línea única de atención al ciudadano 01-8000-114310
 Tel Bogotá: (601) 2201000
 Colombia





Como resultado de la aplicación del instrumento de identificación de la línea base de seguridad del MINTIC, con corte a junio de 2023 y la revisión por parte de auditorías Internas y externas de la Norma ISO 27001:2013, Anexo A con sus 114 Controles de Seguridad y de la evaluación registrada en el modelo de Seguridad y Privacidad de la Información (MSPI) se obtiene un promedio de evaluación de los controles del 70%, para el cierre del 2023, y con el desarrollo de las acciones definidas se pretende avanzar en 5 puntos para llegar a un 75% de avance en la implementación.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	84	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	84	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	92	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	38	100	REPETIBLE
A.10	CRIPTOGRAFÍA	60	100	EFFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	72	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	49	100	EFFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	77	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	37	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	80	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	60	100	EFFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	60	100	EFFECTIVO
A.18	CUMPLIMIENTO	93,5	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		70	100	GESTIONADO

Tabla 2. Evaluación Dominios ISO 27001¹

¹ Fuente: Instrumento de identificación de la línea base de seguridad administrativa y técnica suministrada por MINTIC

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
 Línea única de atención al ciudadano 01-8000-114310
 Tel Bogotá: (601) 2201000
 Colombia





Grafico No.1: Brecha Anexo A. ISO 27001:2013

Se realiza la revisión de los avances en la implementación de los controles definidos por la Norma ISO 27001:2013, Anexo A, en cada uno de los dominios, de lo cual se puede concluir que:

Los dominios que se encuentra en el nivel REPETIBLE requieren establecer las acciones que apoyen la documentación, implementación y operación de los controles y lo lleven a un nivel de madurez superior

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.9	CONTROL DE ACCESO	38	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	37	100	REPETIBLE

Tabla 3. Dominios en estado REPETIBLE

Los dominios que se encuentran en nivel DEFINIDO, requieren la definición de métricas claras sobre los procesos, controles y procedimientos que permitan el seguimiento y control permanente para identificar desviaciones.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.10	CRIPTOGRAFÍA	60	100	DEFINIDO
A.12	SEGURIDAD DE LAS OPERACIONES	49	100	DEFINIDO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	60	100	DEFINIDO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	60	100	DEFINIDO

Tabla 4. Dominios en estado DEFINIDO

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
 Línea única de atención al ciudadano 01-8000-114310
 Tel Bogotá: (601) 2201000
 Colombia





Gobierno del Cambio

Los dominios que se encuentran en nivel ADMINISTRADO, requieren una medición constante de la efectividad de los controles, su monitoreo y seguimiento de tal manera que se garantice su mejora

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	72	100	ADMINISTRADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	77	100	ADMINISTRADO
A.15	RELACIONES CON LOS PROVEEDORES	80	100	ADMINISTRADO
PROMEDIO EVALUACIÓN DE CONTROLES		70	100	ADMINISTRADO

Tabla 5. Dominios en estado ADMINISTRADO

Los dominios que se encuentran en nivel OPTIMIZADO, requieren mantener la constante actualización y permanencia de la operación de los controles de manera que permita su automatización y el mejoramiento continuo.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	84	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	84	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	92	100	OPTIMIZADO
A.18	CUMPLIMIENTO	93,5	100	OPTIMIZADO

Tabla 6. Dominios en estado OPTIMIZADO

Así mismo, el avance general en el ciclo PHVA del Sistema de Gestión de Seguridad y Privacidad de la Información de la Superintendencia alcanzó el 85%, se requiere mantener la actualización periódica de las políticas, los activos y riesgos de seguridad de la información para todos los procesos y la ejecución de los planes de mejora resultado de las auditorías realizadas:

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2023	Planificación	36%	40%
	Implementación	14%	20%
	Evaluación de desempeño	16%	20%
	Mejora continua	18%	20%
TOTAL		85%	100%

Tabla 7. Evaluación ciclo PHVA

Teniendo en cuenta los anteriores resultados, para la vigencia 2023 se establece el Plan de Seguridad y privacidad de la información el cual dando cumplimiento a la Resolución 500 de MINTIC, incluye la Estrategia de Seguridad digital y las acciones requeridas para su implementación y así garantizar la mejora continua.

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
Línea única de atención al ciudadano 01-8000-114310
Tel Bogotá: (601) 2201000
Colombia





6.2. IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (Estrategia de planificación y control operacional)

Dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) soporte del Modelo de Seguridad y privacidad de la información (MSPI) de MINTIC, se han desarrollado, implementado y operado diferentes procedimientos, guías, manuales y formatos que se pueden encontrar en la Intranet de la Superintendencia de Sociedades, con el fin de dar cumplimiento a los controles establecidos en la Norma ISO 27001:2013 Anexo A con sus 114 Controles de Seguridad de la Información, e ir adecuando a la Entidad en la nueva norma ISO 27001:2022 y los requisitos establecidos por la política de Gobierno Digital, la política de Seguridad digital, el FURAG (Formulario único de reporte y avance de Gestión) dentro de los cuales se encuentran:

- Diseño e implementación del curso de seguridad de la información en plataforma MOODLE, cursos de sensibilización presenciales y por TEAMS y emisión de campañas de seguridad por los diferentes medios de comunicación de la Superintendencias de Sociedades.
- El levantamiento de los instrumentos de gestión de la información pública de la Superintendencias de Sociedades se realizó en el último trimestre de 2021 y sobre el cual está prevista su actualización en esta vigencia, para dar cumplimiento a la Ley 1712 de 2014- Ley de transparencia de acceso a la información pública. Estos instrumentos se encuentran publicados en el Portal Web institucional en los siguientes enlaces:

https://supersociedades.gov.co/documents/20122/377715/10.2.1_RegistroActivosInformacion-2021-06-04.xlsx/435f76d7-4046-9331-2dff-7a21fff36274?t=1665337185291

<https://supersociedades.gov.co/documents/20122/377715/Indice-Info-Clasificada-y-Reservada-2021.xlsx/c6aecfaa-ada2-6d1c-7d21-416c1a127669?t=1665755628633>

https://supersociedades.gov.co/documents/20122/377715/10.4.1_EsquemaPublicacionInformacion.xls/e3219284-f4f7-667b-391c-d7246d5d92d6?t=1646925795351

- De acuerdo con la **GC-I-002 INSTRUCTIVO PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**, los activos de información cuya calificación sea ALTA, se le realizará la identificación de riesgos de seguridad de la información, actividad que se encuentra en proceso de actualización.
- Se cuenta con los siguientes documentos que hacen parte de la gestión del Modelo de Seguridad y privacidad de la información de la Superintendencia de Sociedades, los cuales fueron actualizados en su mayoría durante el 2021 y como parte de este plan serán actualizados y publicados en el Sistema de Gestión Integrado.

- ✓ GC-G-002 Guía de Administración de Riesgos
- ✓ GC-I-001 Instructivo para la identificación, clasificación, valoración y etiquetado de activos de información.
- ✓ GC-I-002 Instructivo para la gestión de riesgos de seguridad de la información
- ✓ GC-PO-001 Documento de Políticas del SGI
- ✓ GC-MO-001 Documento de Modelos del SGI
- ✓ GINT-G-005 Guía DRP
- ✓ GINT-G-006 Guía Gestión de Incidentes

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
Línea única de atención al ciudadano 01-8000-114310
Tel Bogotá: (601) 2201000
Colombia



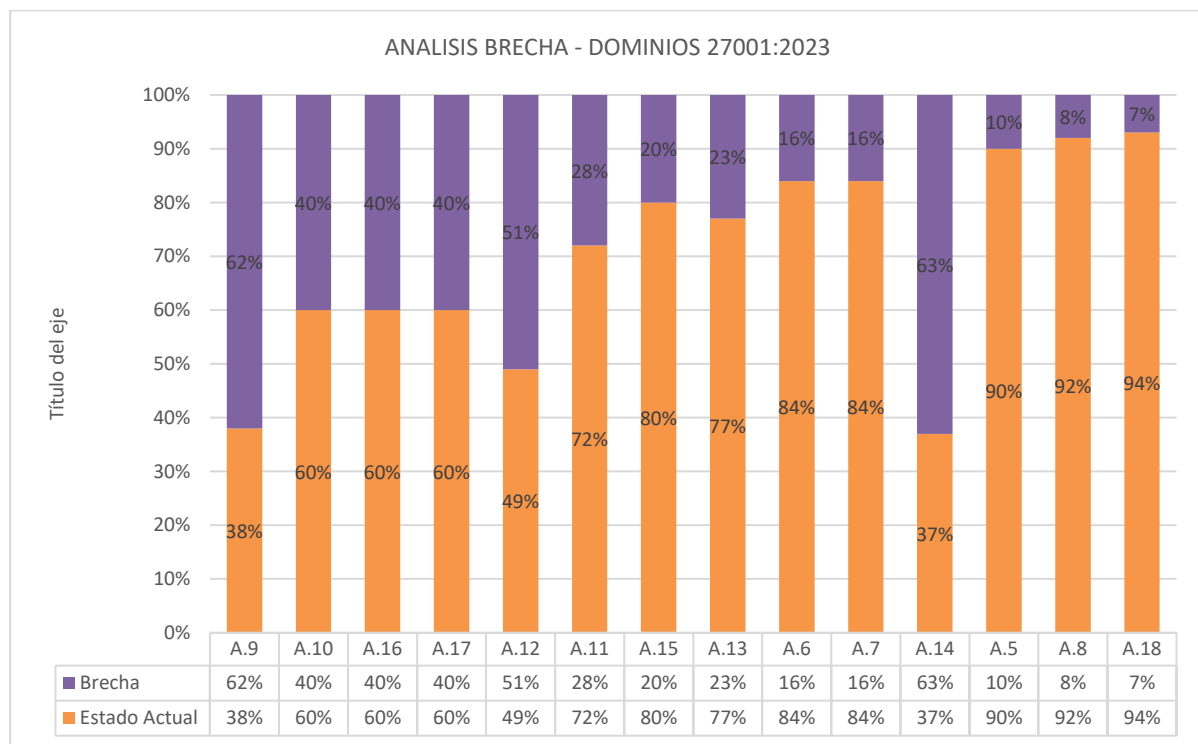


Gobierno del Cambio

- ✓ GINF-PR-006 Cambios al Ambiente Productivo
- ✓ Auditorías internas realizadas por la Oficina de Control Interno.
- ✓ Auditorías externas de Certificación en ISO27001
- ✓ Plan de Seguridad y Privacidad de la Información
- ✓ Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- ✓ Política de tratamiento de datos personales

- El plan de implementación del Sistema de Seguridad y Privacidad de la Información incluye actividades tendientes a aumentar la gestión de cada uno de los dominios y llevarlos a un nivel Optimizado.

Teniendo en cuenta la brecha de los 14 dominios que se muestra en gráfica, se definieron las actividades que hacen parte de la estrategia de planificación y control operacional y que se relacionan a continuación:



Grafica 2. Análisis de Brecha

Para cada uno de los dominios que se encuentra en estado Definido repetible y administrado se definirán actividades tendientes a dar cumplimiento al establecimiento de los controles, según lo expuesto en el numeral 7.1.3. del presente documento.

Los dominios que se encuentra en estado optimizado, serán monitoreados y en lo posible automatizados para garantizar su cumplimiento y actualizados periódicamente para lograr el mejoramiento continuo.

Las estrategias de sensibilización, se definirán en el Plan de Sensibilización en seguridad y privacidad de la información y en conjunto con el PIC Institucional.

La mitigación de los riesgos de seguridad de la información hace parte del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
 Línea única de atención al ciudadano 01-8000-114310
 Tel Bogotá: (601) 2201000
 Colombia





Los activos de información se encuentran en proceso de actualización y luego estarán disponibles para consulta en la página web <https://www.supersociedades.gov.co> en la opción Transparencia y acceso a la información pública - Inicio ([supersociedades.gov.co](https://www.supersociedades.gov.co))

6.3. MATRIZ DE ESTRATEGIA DE PLANIFICACIÓN Y CONTROL OPERACIONAL

CRONOGRAMA						
Dominios ISO 27001	Estado Actual	Nivel	Actividades para lograr los objetivos de SGSI 2023	RESPONSABLE	FECHAS DE PROGRAMACION	
					FECHA INICO	FECHA FINAL
A.5. Políticas de la seguridad de la información	90%	OPTIMIZADO	<ol style="list-style-type: none"> 1. Se debe realizar la actualización y aprobación y divulgación de la política para la seguridad de la Información en la Entidad 2. Se debe realizar la actualización y aprobación y divulgación del documento de modelos y lineamientos para gestión de redes 	DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES	MAYO DE 2023	AGOSTO DE 2023
A.6. Organización de la seguridad de la información	84%	OPTIMIZADO	<ol style="list-style-type: none"> 1. Crear/ actualizar la política para el uso de dispositivos móviles 2. Revisar y actualizar la Política para tele-trabajadores y trabajo en casa 3. Desarrollar el plan de actualización de la documentación del SGSI 4. Realizar la actualización del plan de seguridad y privacidad de la Información para la vigencia 2023 el cual incluye la estrategia de seguridad digital. 5. Aplicar el Instrumento de identificación de la línea base de seguridad administrativa y técnica suministrada por MINTIC. 6. Aplicar instrumento para norma ISO 27001:2022 y definir las acciones para el cierre de brecha 	DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES	ENERO DE 2023	DICIEMBRE DE 2023
A.7. Seguridad de los recursos humanos	84%	OPTIMIZADO	<ol style="list-style-type: none"> 1. Construir el plan de sensibilización en Seguridad de la Información y el esquema de seguimiento 2. Inclusión de los temas de seguridad en el proceso de induccion 3. Inclusión de los temas de seguridad en el proceso de ingreso de contratistas 4. Establecer los lineamientos y el procedimiento para la gestión de los equipos de cómputo, propios de terceros y alquilados 5. Incluir la firma del acuerdo de confidencialidad a todos los usuarios que acceden a la información de la Entidad 	DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES	ENERO DE 2023	DICIEMBRE DE 2023

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
 Línea única de atención al ciudadano 01-8000-114310
 Tel Bogotá: (601) 2201000
 Colombia





CRONOGRAMA

Dominios ISO 27001	Estado Actual	Nivel	Actividades para lograr los objetivos de SGSI 2023	RESPONSABLE	FECHAS DE PROGRAMACION	
					FECHA INICO	FECHA FINAL
A.8. Gestión de activos	92%	OPTIMIZADO	<ol style="list-style-type: none"> Mantener actualizado el instructivo de clasificación de activos, ajustar para dar cumplimiento a Infraestructuras críticas, ley 1712 y datos abiertos. Realizar la actualización anual del registro de activos con cada una de las áreas Realizar la publicación de los instrumentos de la ley 1712 en la página web de la y publicar en datos abiertos Apoyar a los procesos en la identificación de los riesgos de seguridad de la información y la entrega para consolidación en la matriz de riesgos en el sistema correspondiente. Apoyar a los procesos en la implementación de los controles para cada riesgo no aceptable Definir, presentar para aprobación y publicar el plan de tratamiento de riesgos de seguridad y privacidad de la información 	DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES Y ENLACES DE CADA PROCESO	ENERO DE 2023	DICIEMBRE DE 2023
A.9. Control de acceso	38%	REPETIBLE	<ol style="list-style-type: none"> Actualizar la GINT-PR-010 Gestión Usuarios Plataforma Tecnológica Construir los procedimientos para la gestión de perfiles Realizar el levantamiento de perfiles y roles de todos los procesos para las aplicaciones y sistemas de la Superintendencia Implementar el procedimiento de gestión de los perfiles Definir el proyecto de gestión de identidades de la Superintendencia. Realizar la centralización de autenticación a través del DA y realizar la integración de las aplicaciones que lo permitan. Activar el proceso de autogestión de los accesos a través de Microsoft Dar cumplimiento al proceso de monitoreo y custodia de usuarios privilegiados. 	DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES	MARZO DE 2023	DICIEMBRE DE 2023

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
 Línea única de atención al ciudadano 01-8000-114310
 Tel Bogotá: (601) 2201000
 Colombia





CRONOGRAMA

Dominios ISO 27001	Estado Actual	Nivel	Actividades para lograr los objetivos de SGSI 2023	RESPONSABLE	FECHAS DE PROGRAMACION	
					FECHA INICO	FECHA FINAL
A.10. Criptografía	60%	DEFINIDO	1. Validar la política de uso de controles criptográficos y manejo de llaves 2. Realizar el proceso de aseguramiento de los sitios que requieran autenticación a través de certificados digitales 3. Realizar el proceso para la adquisición de los certificados y firmas digitales que se requieran para la operación. 4. Seguimiento a la aplicación de controles criptográficos para la protección de la información	DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES	MARZO DE 2023	DICIEMBRE DE 2023
A.11. Seguridad física y del entorno	72%	GESTIONADO	1. Mejora de controles de acceso y protección contra amenazas en: - Datacenter y centros de cableado - Áreas con servidores, ya sean de procesamiento o dispositivos de comunicación - Áreas donde se encuentren concentrados dispositivos de información - Áreas donde se almacenen y guarden elementos de respaldo datos (CD, Discos, Cintas etc.) 2. Validar el Monitoreo de los controles de accesos biométricos 3. Cumplimiento de normas de seguridad física en centros de datos y de cableado 4. Monitoreo del funcionamiento de las UPS que alimentan el centro de cómputo, y revisar que exista contrato de soporte y mantenimiento	DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES	MAYO DE 2023	DICIEMBRE DE 2023
A.12. Seguridad de las operaciones	49%	DEFINIDO	1. Validar el cumplimiento del GINT-PR-017 Gestión de la capacidad de la infraestructura tecnológica 2. Diseñar en conjunto con la mesa de ayuda el procedimiento de asignación de Equipos que incluya el software y aplicaciones base de los equipos y las políticas de seguridad 3. Diseñar los procedimientos de monitoreo de disponibilidad y seguridad 4. Realizar el monitoreo y análisis de vulnerabilidades detectadas por el Windows defender y otras fuentes como el SOC/NOC, y gestionar su tratamiento tanto para estaciones de trabajo como servidores.	DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES	MARZO DE 2023	DICIEMBRE DE 2023

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
 Línea única de atención al ciudadano 01-8000-114310
 Tel Bogotá: (601) 2201000
 Colombia





CRONOGRAMA

Dominios ISO 27001	Estado Actual	Nivel	Actividades para lograr los objetivos de SGSI 2023	RESPONSABLE	FECHAS DE PROGRAMACION	
					FECHA INICO	FECHA FINAL
			5. Implementar sistema para la gestión de Backups 6. Validar la separación de ambientes (físicos y lógicos) 7. Definir y ejecutar el plan de monitoreo de controles de seguridad 8. Operar y validar la automatización del procedimiento de control de cambios 9. Revisar el cumplimiento de los planes de respaldo de bases de datos y de configuración de servidores 10. Gestionar con la mesa de ayuda y área de infraestructura, la actualización del sistema operativo y antivirus de las estaciones de trabajo a nivel nacional			
A.13. Seguridad de las comunicaciones	77%	GESTIONADO	1. Validar la implementación de IPv4 a IPv6 2. Validar la separación de Redes (segmentación) actualizar la documentación existente 3. No se cuenta con control de acceso a la red a través de NAC 4. Validar los lineamientos de la política respecto a acceso, revisar la inactivación de estos servicios corporativos y servicios de red 5. Ajustar el servicio de correo (borrado) e internet dentro de las políticas y realizar la divulgación	DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES	MARZO DE 2023	DICIEMBRE DE 2023
A.14. Adquisición, desarrollo y mantenimiento de sistemas	37%	REPETIBLE	1. Revisar que los contratos para desarrollo de software incluyan el cumplimiento de principios de desarrollo seguro. 2. Realizar la actualización del procedimiento para que se incluyan los requisitos de seguridad y los controles en el ciclo de vida de desarrollo. 3. Se debe realizar la actualización del Inventario de Aplicaciones para que sea la base para la construcción del catálogo de Servicios, e incluir los esquemas de backups para esta información. 4. Realizar análisis de código estático y dinámico de SW y realizar el proceso de mitigación antes de salida a producción	DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES	MARZO DE 2023	DICIEMBRE DE 2023

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
 Línea única de atención al ciudadano 01-8000-114310
 Tel Bogotá: (601) 2201000
 Colombia





CRONOGRAMA

Dominios ISO 27001	Estado Actual	Nivel	Actividades para lograr los objetivos de SGSI 2023	RESPONSABLE	FECHAS DE PROGRAMACION	
					FECHA INICO	FECHA FINAL
A.15. Relaciones con los proveedores	80%	GESTIONADO	<ol style="list-style-type: none"> 1. Actualizar la política de seguridad de la información para proveedores y terceras partes. 2. Monitoreo al cumplimiento de procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, los incidentes de seguridad de la información y la revaloración de los riesgos. 3. Verificar que los proveedores diligencien el acuerdo de confidencialidad 	DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES	MARZO DE 2023	JUNIO DE 2023
A.16. Gestión de incidentes de seguridad de la información	60%	DEFINIDO	<ol style="list-style-type: none"> 1. Realizar la revisión, ajustes y actualización de la guía de Gestión de Incidentes 2. Verificar que las gestiones de incidentes de seguridad de la Información estén debidamente documentadas en la mesa de servicio con el diligenciamiento de las lecciones aprendidas. 3. Realizar la capacitación en las actividades de gestión de incidentes de seguridad 4. Definir las guías de atención para los incidentes comúnmente presentados - playbooks 5. Realizar la definición y medición del procedimiento a través de los indicadores 6. Se deben realizar los procesos de retroalimentación adecuados para asegurar que las personas que reportan eventos de seguridad de la información sean notificadas de los resultados después de que la cuestión haya sido tratada y cerrada. 	DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES E INFORMATICA	ENERO DE 2023	DICIEMBRE DE 2023

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
 Línea única de atención al ciudadano 01-8000-114310
 Tel Bogotá: (601) 2201000
 Colombia





CRONOGRAMA

Dominios ISO 27001	Estado Actual	Nivel	Actividades para lograr los objetivos de SGSI 2023	RESPONSABLE	FECHAS DE PROGRAMACION	
					FECHA INICO	FECHA FINAL
A.17. Aspectos de seguridad de la información de la gestión de continuidad de negocio	60%	DEFINIDO	<ol style="list-style-type: none"> 1. Actualización de los Planes de Contingencia tecnológica para cada uno de los servicios. 2. Actualización Planes de recuperación ante desastres (DRP) 3. Revisión de Sistemas de alta disponibilidad para los procesos críticos 4. Revisión de la seguridad para la estrategia de contingencia definida 5. Verificar la disponibilidad de créditos en la nube para respaldo de bases de datos y configuraciones de servidores 6. Verificar que se esté llevando a la nube de "azure" las copias de respaldo 	DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES	JULIO DE 2023	DICIEMBRE DE 2023
A.18. Cumplimiento	93.5%	OPTIMIZADO	<ol style="list-style-type: none"> 1. Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información- Actualización Normograma 2. Actualización de las políticas para el cumplimiento de los requisitos y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. 3. Ejecutar el plan de acción definido como resultado de la auditoria de derechos de autor sobre el cumplimiento de derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos, esta política debe estar orientada no solo al software, sino también a documentos gráficos, libros, etc. 4. Monitoreo del cumplimiento de la instalación de software 5. Monitoreo al inventario de software instalado y se compara con el número de licencias adquiridas para asegurar que no se incumplen los derechos de propiedad intelectual. 6. Hacer seguimiento a los hallazgos, acciones correctivas y oportunidades de mejora de las evaluaciones y auditorias de seguridad realizadas por el ente certificador y control interno 	DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES	MARZO DE 2023	DICIEMBRE DE 2023

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
 Línea única de atención al ciudadano 01-8000-114310
 Tel Bogotá: (601) 2201000
 Colombia





6.4. ESTRATEGIA DE SEGURIDAD DIGITAL

Durante el primer cuatrimestre de 2023, con el acompañamiento de un fabricante líder en soluciones y servicios de ciberseguridad, se realizó la evaluación del marco de Referencia de NIST para Ciberseguridad arrojando los siguientes resultados los cuales permiten realizar la identificación de las brechas de cumplimiento en cada una de las aristas que conforman el marco de referencia de NIST.

La evaluación fue realizada bajo los siguientes dominios que define el Marco de Referencia de NIST para Ciberseguridad:

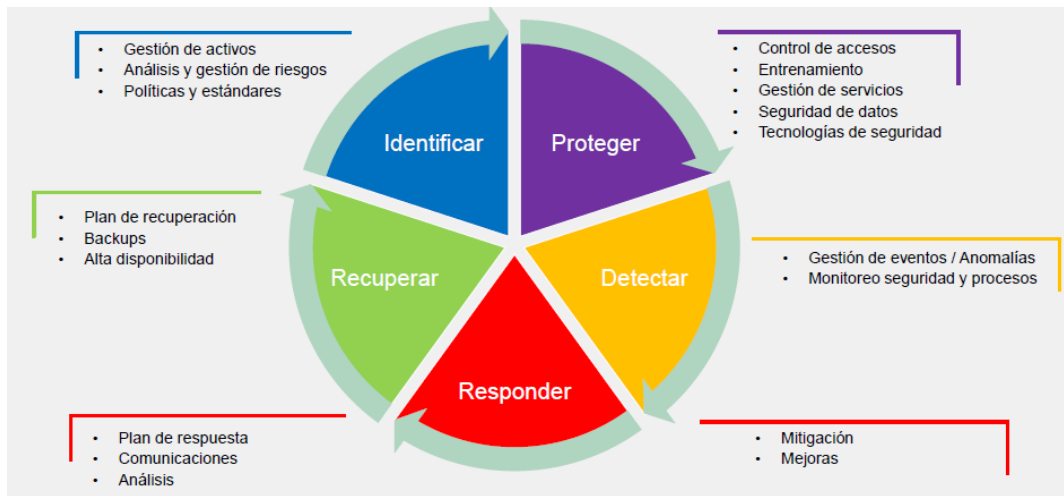


Imagen No.1 marco de referencia NIST

Y de acuerdo con los siguientes niveles de madurez*:

PONDERACION		DESCRIPCION
0%	1- INEXISTENTE	Falta total de un proceso reconocible. La organización ni siquiera ha reconocido que hay un problema que resolver.
33%	2-INCIAL	Este proceso es manual y tiene un cubrimiento muy básico
66%	3-DEFINIDO	Este proceso esta Automatizado por medio de una herramienta tecnológica y tiene un cubrimiento parcial
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

Dando como resultado general, en la sumatoria de los dominios evaluados (identificar, proteger, detectar, responder y recuperar), un puntaje medio-bajo de 40,85%, frente a las demás entidades públicas, el puntaje de la Superintendencia está actualmente situada dentro del promedio en el que se encuentran las demás entidades, con una calificación media –baja (45%-50%).

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
Línea única de atención al ciudadano 01-8000-114310
Tel Bogotá: (601) 2201000
Colombia





MADUREZ 40.85

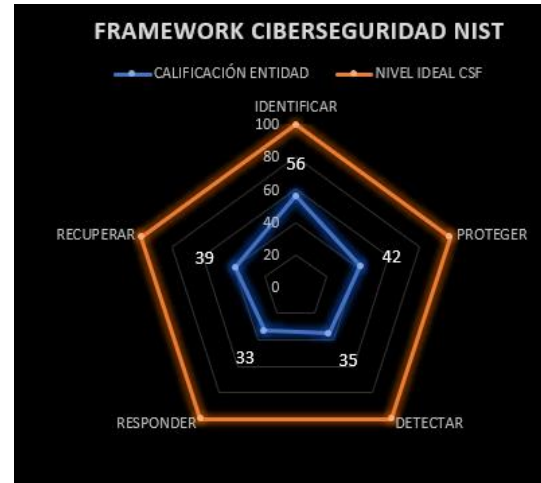


Imagen No.2 Calificación marco de referencia NIST

De acuerdo con el resultado obtenido a continuación se relacionan las brechas identificadas para cada uno de los dominios:

Se realizó la medición de las mejores prácticas de Ciberseguridad (NIST) incluidas en el instrumento de medición de MINTIC y dentro de los aspectos que requieren revisión permanente para garantizar la implementación de la política de seguridad digital obteniendo un puntaje promedio de 41% de cumplimiento con los siguientes resultados para cada dominio:

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
DOMINIO	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	56	100
PROTEGER	42	100
DETECTAR	35	100
RESPONDER	33	100
RECUPERAR	39	100

Tabla 7. Evaluación Modelo Ciberseguridad NIST

6.4.1. DOMINIO IDENTIFICAR

Se obtuvo una calificación de 56%, fue la más alta de los dominios evaluados, este resultado obedece al esfuerzo que se ha hecho desde la DTIC por tener actualizados las políticas, procesos, procedimientos y guías referentes a la gestión en seguridad.

Este dominio cubre los controles establecidos en la Norma ISO 27001:2013 relacionados con:

- Políticas de seguridad
- Gestión de activos
- Organización de la seguridad
- Gestión de Riesgos de Seguridad



RECOMENDACIONES:

Se recomienda aumentar la inteligencia de amenazas de los controles de seguridad mediante la integración con fuentes externas y actualización dinámica de políticas.

Se recomienda mejorar y automatizar los mecanismos de identificación y clasificación de activos con el fin de hacer una evaluación correcta de los riesgos asociados a los diferentes componentes de la infraestructura y la información de la entidad.

Se recomienda implementar mecanismos de confidencialidad de la información mediante el cifrado y ofuscación de datos en reposo y firewall de base de datos.

Se recomienda implementar mecanismos de prevención de fuga de información para proteger la divulgación de información sensible.

6.4.2. DOMINIO PROTEGER

Para el dominio proteger se obtuvo una calificación de 42%, este resultado obedece a la ausencia de controles de seguridad para el acceso remoto, múltiples factores de autenticación, controles para la protección de la integridad de los datos en reposo y controles para la fuga de información.

Este dominio cubre los controles establecidos en la Norma ISO 27001:2013 relacionados con:

- Control de Accesos
- Entrenamiento
- Gestión de Servicios
- Seguridad de Datos
- Tecnologías de Seguridad

RECOMENDACIONES

Se recomienda fortalecer la seguridad de las aplicaciones implementando mecanismos de autenticación fuerte (2FA) en los accesos VPN y aplicaciones misionales.

Se recomienda implementar tecnologías de validación de postura (evaluación de los requisitos de seguridad para la conexión a la red, permitir o no el acceso) para los usuarios conectados tanto a la red local como a través de VPN.

Se recomienda realizar el monitoreo de los eventos críticos de las Bases de Datos a través de mecanismos como el SIEM.

Realizar la definición y activación a través del Firewall de los módulos de DLP.

6.4.3. DOMINIO DETECTAR

Para el dominio de detectar se obtuvo una calificación de 35%, Se debe contar con el servicio de Monitoreo Continuo (NOC / SOC), con el fin de realizar la detección de anomalías y eventos maliciosos y los procesos de detección

RECOMENDACIONES

Se recomienda implementar monitoreo NOC / SOC unificando la visibilidad a nivel de infraestructura y

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
Línea única de atención al ciudadano 01-8000-114310
Tel Bogotá: (601) 2201000
Colombia





Gobierno del Cambio

controles de seguridad tanto en premisas como en nube, apoyado en herramientas de SIEM y SOAR de nueva generación, definiendo a la vez una política de retención de logs.

Se recomienda complementar la detección de los controles actuales con análisis y protección de amenazas avanzadas y de día cero basadas en inteligencia artificial.

Se recomienda implementar mecanismos de monitoreo de comportamiento de usuarios, con el fin de detectar posibles brechas de seguridad al interior de la organización (publicación de datos, instalación de software)

Se debe realizar los ajustes al procedimiento de incidentes y definir los procesos requeridos para la detección, reglas de correlación y eventos.

Se debe realizar el monitoreo y acciones sobre las herramientas con las que se cuenta actualmente, y realizar el análisis de malware.

Integrarse con Office 365 para conocer los movimientos que se realizan de manera automatizada.

Se requiere validar y activar la protección de amenazas de día cero con el EDR actual.

Validar el Sand Boxing Cloud (tráfico actual del firewall http y https) con el que se cuenta actualmente a través del Firewall.

6.4.4. DOMINIO RESPONDER

Para el dominio de responder se obtuvo una calificación de 33%, este resultado obedece a que existen un plan de respuesta a incidentes.

RECOMENDACIONES

Se recomienda implementar dentro del NOC / SOC de la entidad, mecanismos de investigación de incidentes, que permitan a la entidad lograr tener un mejor contexto de los ataques y las campañas de ciberdelincuentes a nivel mundial.

Se recomienda implementar dentro del NOC / SOC mecanismos de protección de marca y gestión de riesgo digital, con el fin de contar con mecanismos de detección temprana de ataques que afecten la reputación e imagen de la entidad, y que permitan la toma de contramedidas contra los mismos.

Se recomienda implementar mecanismos de respuesta automatizada a eventos de ciberseguridad, con el fin de disminuir los tiempos de afectación y simplificar la operación de los administradores.

Se recomienda actualizar el procedimiento existente y definir claramente el proceso de comunicación análisis y mitigación, definir niveles de atención de los incidentes presentados y la articulación con los demás procesos de la Entidad.

Validar la configuración del EDR, frente a la respuesta de los incidentes, definir las acciones de bloqueo.

6.4.5. DOMINIO RECUPERAR

Para el dominio de responder se obtuvo una calificación de 39%, se tienen definidos planes de recuperación para algunos servicios.

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
Línea única de atención al ciudadano 01-8000-114310
Tel Bogotá: (601) 2201000
Colombia





RECOMENDACIONES

Se recomienda implementar dentro del NOC / SOC de la entidad, mecanismos de enriquecimiento de base de datos de lecciones aprendidas, que permita tener playbooks de acción afinados para la ocurrencia de eventos similares, que optimicen el tiempo de respuesta de la entidad.

Se recomienda hacer validación periódica de los respaldos de información y procesos de restauración con el fin de estar preparados ante la ocurrencia de eventos de ciberseguridad o de otra índole.

Se recomienda definir los mecanismos de respaldo entre datacenter incluyendo premisas y nube, y su prueba periódica.

Definir las pruebas del proceso de restauración de los esquemas de contingencia, para los servicios tecnológicos de la Entidad.

Actualizar el plan de Recuperación ante desastres y desarrollar las pruebas correspondientes.

Se debe contar con playbooks debidamente documentados y disponibles para la atención de los incidentes que se presenten.

HOJA DE RUTA CIBERSEGURIDAD

NIST	ESTRATEGIA	CORTO PLAZO	MEDIANO PLAZO	LARGO PLAZO	TECNOLOGIA y/o PROCESO
IDENTIFICAR	<p>I.a) Identificar, gestionar y gobernar los riesgos de ciberseguridad relacionados a los procesos de la entidad, enfatizando en los riesgos propios en la cadena de suministro y los riesgos asociados a los servicios en nube.</p> <p>I.b) La entidad debe identificar y mantener contacto con las autoridades de autoridad correspondientes y expedir normas para la protección de los servicios esenciales, relacionado con la infraestructura crítica.</p>	I.b1, Ia2	I.a1, Ia2		<p>I.a1) Debe construirse una política para el cumplimiento de ciberseguridad en la relación con los proveedores, se debe exigir cláusulas contractuales para el cumplimiento de los controles mínimos de seguridad digital en proveedores y la totalidad de la cadena de suministro.</p> <p>I.a2) Los riesgos de seguridad digital asociados a los servicios en la nube deben identificarse y gestionarse.</p> <p>I.b1) Mantener contacto con el enlace de seguridad digital dispuesto por el CSIRT Gobierno, gestionar alarmas, boletines del sector, incluir el servicio de monitoreo de disponibilidad del portal web que realiza el CSIRT Gobierno</p>

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
 Línea única de atención al ciudadano 01-8000-114310
 Tel Bogotá: (601) 2201000
 Colombia





HOJA DE RUTA CIBERSEGURIDAD

NIST	ESTRATEGIA	CORTO PLAZO	MEDIANO PLAZO	LARGO PLAZO	TECNOLOGIA y/o PROCESO
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">PROTEGER</p>	<p>P.a) Seguir madurando en la protección del control de acceso a la red, adquirir, implementar y/o potencializar tecnologías.</p> <p>P.b) Avanzar en la protección de los datos en sus estados (reposo, transporte y procesamiento).</p> <p>P.c) Madurar en los procesos de aseguramiento y gestión de vulnerabilidades del ambiente tecnológico.</p> <p>P.d) Avanzar en la protección del entorno.</p>	<p>P.a1, P.a3</p>	<p>P.a2, P.a4, P.b2, P.c2, P.c3, P.c4, P.d1,</p>	<p>P.b1, P.c1, P.d2, P.d3, P.d4</p>	<p>P.a1) Potencializar las bondades del MFA que actualmente provee Microsoft para proteger con doble autenticación el acceso a la VPN, portales en nube y demás necesidades que se puedan evaluar con el proveedor, así como poder desplegar un servidor de MFA para autenticación onpremise, con el objetivo de gobernar la protección de la identidad con una sola solución (Microsoft).</p> <p>P.a2) Adquisición de una solución de protección de acceso a la red y cero confianza, para evaluar la postura en seguridad de los dispositivos que tienen acceso a la red y la visión y control de los mismos.</p> <p>P.a3) Se debe habilitar el port security a todos los puertos de los switches de acceso, con un máximo de (2) MAC permitidas, se deben deshabilitar los puertos que no se estén utilizando (administrative Down).</p> <p>P.a4) Realizar la identificación de roles y privilegios en los sistemas de información con el objetivo de gobernar el menor privilegio.</p> <p>P.b1) Adquirir y/o acoger una tecnología de cifrado-ofuscamiento para los datos en reposo (bases de datos).</p> <p>P.b2) Implementar políticas para la prevención de fugas de información (DLP) de la entidad mediante el etiquetado de la información aprovechando las características de la licencia E5 (Microsoft).</p> <p>P.c1) Adquisición de herramienta y/o servicios tecnológicos que evalúen, auditen el estado del aseguramiento (hardening) de los sistemas de información mediante líneas base.</p> <p>P.c2) Adquisición de herramientas y/o servicios tecnológicos que evalúen el código estático - dinámico de los sistemas de información misionales de la entidad</p> <p>P.c3) Adquisición de herramientas y/o servicios tecnológicos para el descubrimiento de vulnerabilidades en</p>

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
 Línea única de atención al ciudadano 01-8000-114310
 Tel Bogotá: (601) 2201000
 Colombia





HOJA DE RUTA CIBERSEGURIDAD

NIST	ESTRATEGIA	CORTO PLAZO	MEDIANO PLAZO	LARGO PLAZO	TECNOLOGIA y/o PROCESO
					<p>activos TI y aplicaciones web.</p> <p>P.c4) Construcción de procesos, políticas, planes para el aseguramiento tecnológico que permitan controlar (P.c1,P.c2,P.c3).</p> <p>P.d1) Adquisición de soluciones perimetrales específicas de seguridad para el ambiente en nube para la protección de infraestructura y aplicaciones.</p> <p>P.d2) Adquisición de soluciones de protección orientadas a la micro segmentación en ambientes virtualizados.</p> <p>P.d3) Arquitectura segmentada en ISFW (Internal Segmentation Firewall), beneficios en visibilidad de eventos en la red interna.</p> <p>P.d4) Adquisición de un escudo de protección para los ataques de denegación de servicio, se recomienda en nube lo más cerca al origen del ataque.</p>
DETECTAR	<p>D.a) Monitoreo de amenazas y comportamientos sospechosos.</p> <p>D.b) Construcción, actualización de planes técnicos, procedimentales para la temprana contención de un ataque.</p> <p>D.c) Visión y cacería de amenazas del comportamiento en la red</p> <p>D.d) Detección inteligente de ataques (objetivos, comportamientos, tecnologías y métodos)</p>	<p>D.a1, D.a2, D.b2</p>	<p>D.a1, D.a2, D.b2, D.c1</p>	<p>D.a1, D.a2, D.b2, D.d1</p>	<p>D.a1) Adquisición de herramientas tecnológicas y/o servicios para la correlación de registros y monitoreo, visibilidad y alertamiento de posibles incidentes en los ambientes tecnológicos (hube, en premisa) y las marcas de la entidad (redes sociales, dominios, aplicaciones, código, etc.) - SOC-NOC</p> <p>D.a2) Implementar las características de correlación que trae el producto de SENTINEL, incluido en el licenciamiento E5 de Microsoft en tiempos en los que D.a1) no está disponible por cualquier que sean los motivos.</p> <p>D.b2) Construcción, actualización y socialización de playbooks con y sin servicios SOC-NOC.</p> <p>D.c1) Adquisición de una tecnología de detección y respuesta para el comportamiento de la red NDR.</p> <p>D.d1) Adquisición, gestión de una estrategia honeypot y sandboxing.</p>

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
 Línea única de atención al ciudadano 01-8000-114310
 Tel Bogotá: (601) 2201000
 Colombia





HOJA DE RUTA CIBERSEGURIDAD

NIST	ESTRATEGIA	CORTO PLAZO	MEDIANO PLAZO	LARGO PLAZO	TECNOLOGIA y/o PROCESO
RESPONDER	<p>RS.a) Avanzar en la construcción de un plan de respuesta.</p> <p>RS.b) Simulación de ataques, puesta en marcha al plan de respuesta a incidentes de ciberseguridad.</p> <p>RS.c) Soluciones en detección y respuesta.</p>	RS.a1, RS.b1	RS.b1, RS.c2	RS.b1, RS.c1	<p>RS.a1) Construcción del plan de respuesta a incidentes de ciberseguridad, el cual debe incluir los roles, responsables e implícitamente el plan de comunicaciones en la entidad y con las entidades de autoridad.</p> <p>RS.b1) Realizar ejercicios de simulación de ciberataques en donde se realicen ejercicios de salas de crisis y análisis forense, el resultado de estos debe socializarse a la dirección y deben tenerse en cuenta las lecciones aprendidas.</p> <p>RS.c1) Adquisición de herramientas tecnológicas en una solución estratégica de detección y respuesta (XDR) que tenga la capacidad de alimentarse del D.a1 y automatizar procesos de respuesta.</p> <p>Rs.c2) Adquisición de características de SOAR en el D.a1 para la automatización de configuraciones a los casos de uso establecidos</p>
RECUPERAR	<p>RC.a) Plan de recuperación ante desastres tecnológicos DRP.</p> <p>RC.b) Estrategias de recuperación.</p> <p>RC.c) Balanceo de canales y aplicaciones</p>	RC.a1, RC.a2, RC.b1	RC.a1, RC.a2, RC.b1, RC.c1	RC.c2	<p>RC.a1) Apoyar la construcción de un plan DRP.</p> <p>RC.a2) Los controles de seguridad definidos en el ambiente DRP, deberán obedecer a los mismos del ambiente original.</p> <p>RC.b1) Definir cronograma para ejercicios de recuperación en: contingencia de canales, backups en línea y en cinta, balanceo de aplicaciones, los que apliquen, tomar lecciones aprendidas.</p> <p>RC.c1) Adquisición/implementación de tecnología SDWAN para contingencia en canales, con el objetivo de aprovechar los canales de internet, VPN y MPLS de la Superintendencia.</p> <p>RC.c2) Adquisición de tecnologías para el balanceo global por servidor de nombres (GSLB) con el objetivo de balancear aplicaciones en los ambientes dispuestos de la superintendencia.</p>

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
 Línea única de atención al ciudadano 01-8000-114310
 Tel Bogotá: (601) 2201000
 Colombia





7. RECURSOS

La implementación del Plan de Seguridad y Privacidad de la Información, se realizará con recursos propios con funcionarios del Grupo de Seguridad e Informática Forense y del proyecto de inversión para el fortalecimiento del modelo de operación interno de la Dirección de Tecnología de la Información y las Comunicaciones para la implementación de la política de Gobierno Digital.

8. SEGUIMIENTO Y MEDICIÓN

El monitoreo y seguimiento interno al cumplimiento de las actividades del plan definidas en el cronograma de manera mensual y presentar trimestralmente el resultado al comité institucional de gestión y desempeño (CIGD).

8.1. INDICADORES

La medición se realiza con el indicador “Cumplimiento implementación y mantenimiento del MSPI”, que está orientado principalmente a la mejora del modelo de seguridad y privacidad de la información. Para este fin, se utilizará el Instrumento de identificación de la línea base de seguridad, proporcionado por el Ministerio de Tecnologías de la Información y las Comunicaciones.

$$\text{Porcentaje de optimización del SGSI} = \frac{\text{Porcentaje de cumplimiento del MSPI}}{\text{Meta de Cumplimiento programada para el MSPI}}$$

Adicionalmente, se tendrá en cuenta el indicador de cumplimiento FURAG para la política de Seguridad de la Información. Actualmente el indicador FURAG se encuentra en:



Para la mejora de este indicador, la función pública indica algunas actividades a desarrollar, que quedan registradas en el plan de mejoramiento FURAG, supervisado por la Oficina Asesora de Planeación.

Otro de las mediciones para el avance en la implementación del Modelo de Seguridad y privacidad de la información tiene que ver con el cumplimiento de los requisitos y controles del anexo A de la

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
Línea única de atención al ciudadano 01-8000-114310
Tel Bogotá: (601) 2201000
Colombia





Gobierno del Cambio

Norma ISO 27001:2013, Para esto las auditorías internas y externas dejan informes con las observaciones y hallazgos, los cuales, según los lineamientos del Sistema de Gestión Integrado, deben generar un plan de mejoramiento.

Finalmente, se medirá el cumplimiento del presente Plan, a través del resultado del siguiente indicador, para el cual la meta es 80%:

Cumplimiento plan de seguridad y privacidad de la Información: Actividades Ejecutadas
Actividades Programadas

En la Superintendencia de Sociedades trabajamos para contar con empresas competitivas, productivas y perdurables y así generar más empresa, más empleo.

www.supersociedades.gov.co
webmaster@supersociedades.gov.co
Línea única de atención al ciudadano 01-8000-114310
Tel Bogotá: (601) 2201000
Colombia

