COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Tecnologías y Sistemas de Información
Coordinador: Ingrid Picón Carrascal.
Líder: Leidy Diana Rojas Garzón.

Enero de 2020

CONTENIDO

Historia de Actualizaciones

Fecha	Descripción	Responsable
Enero -2020	Creación Plan Estratégico Seguridad y Privacidad de la Información	CISO

1. INTRODUCCIÓN

La seguridad y privacidad de la información en las entidades busca afrontar los retos que impone el negocio en la incursión de nuevas infraestructuras digitales modernas, robustas y seguras.

Teniendo en cuenta el acelerado avance de las tecnologías de información y comunicaciones, genera preocupación e incertidumbre el manejo de los riesgos de la información que estén asociados con las debilidades en la seguridad de las tecnologías de la información, vulnerabilidades que puedan afectar a los activos de información, los cuales pueden ocasionarse por el manejo de una ciberseguridad inadecuada afectando la triada de la seguridad de la información como lo son: la disponibilidad, confidencialidad e integridad.

Con el fin de garantizar la seguridad de la información en las entidades públicas y privadas, se deben desarrollar capacidades que les permita estar un paso adelante de las amenazas y vulnerabilidades latentes que a diario atentan en contra de los activos de información, infraestructuras críticas y los usuarios, estos como agentes del ciberespacio.

Actualmente la Comisión de Regulación de Comunicaciones - CRC tiene el propósito de fortalecer la protección de los activos de información que soportan los procesos de la Entidad y apoyan la implementación del Modelo de Seguridad y Privacidad de la Información.

La Comisión de Regulación de Comunicaciones, para asegurar la dirección estratégica de la Entidad, establece la política de seguridad de la información con los siguientes objetivos de seguridad de la información:

- ✓ Minimizar el riesgo de los procesos misionales de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Cumplir con los principios de la función administrativa.
- ✓ Mantener la confianza de los funcionarios, contratistas y terceros.
- ✓ Apoyar la innovación tecnológica.
- ✓ Implementar el sistema integral de gestión en el aparte de seguridad de la información
- ✓ Proteger los activos de información.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Comisión de Regulación de Comunicaciones. (Rojas, D. (2016). Política General de Seguridad de la Información de la CRC, p.3)

De acuerdo con el estado actual en la Comisión de Regulación de comunicaciones, existe la necesidad de diseñar un Plan Estratégico de Seguridad y Privacidad de la Información que fortalezca las políticas de seguridad de la información y su gestión antes de posibles fallas en los procesos y la responsabilidad en el manejo de los

procedimientos al interior de la entidad, minimizando las potenciales amenazas que pueden ser introducidas accidental o deliberadamente.

Teniendo en cuenta lo anterior, La Coordinación de Tecnologías y Sistemas de Información de la Comisión de Regulación de Comunicaciones plantea presentar el análisis de la información referente a temas de seguridad y privacidad de la información, diseñando un Plan Estratégico de Seguridad y Privacidad de la Información basado en los estándares de la ISO 270001, el Modelo de Seguridad y Privacidad de la Información por MinTIC y lineamientos de Gobierno Digital con el fin de proporcionar una solución a los requerimientos de seguridad y protección de la información en la Entidad, fortaleciendo así las políticas de seguridad existentes, prevenir posibles daños o perdida de información y afianzando la cultura de seguridad de la información entre los funcionarios.

La importancia del apoyo de la alta dirección para la implementación del componente de Seguridad y Privacidad de la información y la gestión de los riesgos de Seguridad de la información en la Entidad con respecto a lo indicado, toma relevancia al formular un Plan estratégico de Seguridad y Privacidad de la Información para que de forma estructurada se establezcan las iniciativas y proyectos que garanticen el cumplimiento del objetivo de seguridad de la información que es proteger, asegurar y minimizar el daño en el que pueda incurrir la entidad y que afecte sus activos de información.

Los proyectos que componen un Plan Estratégico de seguridad y privacidad de la información varían en función de diversos factores relacionados como:

- El tamaño de la Organización
- El nivel de Madurez en tecnología
- El sector al que pertenece la empresa
- El contexto legal que regula las actividades de esta
- La naturaleza de la información que manejamos
- El alcance del proyecto
- Otros aspectos organizativos

2. OBJETIVO

La formulación del Plan Estratégico de Seguridad y Privacidad de la Información de la Comisión de Regulación de Comunicaciones (CRC) se enmarca en los siguientes objetivos:

- Realizar un diagnóstico de la situación actual de la seguridad y privacidad de la información en la Entidad.
- Definición de proyectos e iniciativas.
- Clasificar y priorizar los proyectos a realizar.
- Aprobar el Plan de Seguridad y Privacidad de la Información
- Puesta en marcha del plan.

3. ALCANCE DEL DOCUMENTO

Este documento incorpora la definición estratégica de la Seguridad y Privacidad de la información para la Coordinación de Tecnologías de Información y Comunicaciones,

estableciendo el plan de implementación de los proyectos y servicios que se proponen ejecutar en el año 2020, definidos a través del plan de acción de la entidad para los diferentes ámbitos en el Modelo de Seguridad y privacidad de la información.

Adicionalmente, como resultado de los ejercicios incorpora el plan de acción a través de la definición de la hoja de ruta.

El documento describe las definiciones realizadas sobre la estrategia, objetivos, marco normativo, situación actual, entendimiento estratégico, modelo de gestión y el respectivo el modelo de planeación definiendo el portafolio de proyectos y la hoja de ruta de implementación.

El desarrollo de las definiciones mencionadas se describe en los capítulos a continuación.

4. MARCO NORMATIVO

Normativa	Descripción General
Ley 527 de 1999	Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones.

Normativa	Descripción General
Decreto 103 de 2015	Reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Ley 1712 de 2014	Crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1581 de 2012	Dicta disposiciones generales para la protección de datos personales.
Ley 1341 de 2009	Definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones
Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 de 2012.
Decreto 2573 de 2014	Establece los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Ley 1955 de 2019	Por la cual se expide el Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, pacto por la equidad".
Decreto 1078 de 2015	Marco de Referencia de Arquitectura Empresarial para la gestión de TI (Artículo 2.2.5.1.2.2)
Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
Decreto 415 del 7 de marzo de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los

Normativa	Descripción General
	lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones
Decreto 1413 del 25 de agosto de 2017	Por el cual presente reglamenta parcialmente el Capítulo IV del Título 111 de la Primera Parte de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo los lineamientos que se deben cumplir para la prestación de servicios ciudadanos digitales, y para permitir a los usuarios el acceso a la administración pública a través de medios electrónicos
Decreto 612 del 4 abril de 2018	Por el cual Adicionar al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, los siguientes artículos: "2.2.22.3.14. **Integración de los planes institucionales y estratégicos al Plan de** Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011
Decreto 1008 del 14 junio de 2018	Por el cual estable el Objeto. El presente capítulo establece lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.

Tabla 1 - Marco normativo Plan Seguridad y Privacidad de la información.

Resumen de aplicación del Marco Normativo.

Resolución No. 003484 de 2012 por la cual se crea el Sistema de Información integral del sector TIC-Colombia TIC, en el artículo 2° Entidades públicas de conforman el sistema Colombia TIC y sus responsabilidades. La Comisión de Regulación de comunicaciones hace parte del sistema Colombia TIC. (Comunicaciones, M. de T. de la I. y las (2012). Resolución 003484 MinTIC. Retrieved from https://www.mintic.gov.co/portal/604/articles-3789_documento.pdf)

De acuerdo con lo dispuesto en el artículo 4 de la Ley de 2009, es función del estado invertir en el sector de las Tecnologías de la información y las comunicaciones TIC, para promover condiciones de seguridad del servicio al usuario final, incentivando acciones de prevención de fraudes en la red, así como la seguridad informática y de redes.

Decreto 1008 de 14 de junio de 2018 por el Ministerio de tecnologías de la información y las comunicaciones, en el **artículo 2.2.9.1.1.1** Objeto. El presente capitulo establece lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las Comunicaciones para consolidad un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.

En el **artículo 2.2.9.1.1.3** Principios, en este se encuentra Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riegos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades de Estado, y de los servicios que presentan al ciudadano.

Como Habilitadores transversales de la Política de Gobierno Digital: Son los elementos fundamentales de **Seguridad de la Información**, Arquitectura y servicios ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Los propósitos de la Política de Gobierno Digital que están relacionados con seguridad de la información son los siguientes:

- Habilitar y mejorar la provisión de servicios digitales de confianza y calidad
- Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información. (Comunicaciones, M. de T. de la I. y las. (2018). Decreto 1008 14jun 2018 MinTIC, 1–7).

La elaboración del Plan Estratégico de Seguridad y Privacidad de la Información se construirá siguiendo los principales marcos de referencia en materia de seguridad (ISO 27001, 27002, MSPI de Ministerio de tecnologías de información y comunicaciones) y

lineamientos establecidos en Gobierno Digital. (ICONTEC. (2013). Tecnología De La Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información (Sgsi). Requisitos Ntc-Iso/Iec 27001. *Icontec*, 37)

5. ANÁLISIS DE LA SITUACIÓN ACTUAL

En este apartado se describe la situación actual de la seguridad y privacidad de la información de la entidad en relación con los dominios del modelo de Seguridad y Privacidad de la Información del MinTIC. Este análisis debe permitir conocer el estado actual o línea base a partir de la cual se debe partir para proyectar la visión de lo que se espera en materia de gestión de seguridad de la información en la entidad.

Los resultados de cada análisis muestran el estado en cuanto al cumplimiento del modelo y un análisis cualitativo representado porcentualmente, que indica a su vez las brechas a cerrar y que son determinantes para el modelo de planeación y la inclusión dentro del portafolio de proyectos.

Respecto a la cuantificación y a los criterios de calidad definidos, y de acuerdo con el autodiagnóstico de los componentes de Gobierno Digital para el componente trasversal de Seguridad y privacidad de la información.

Anexo: Instrumento Autodiagnóstico MSPI

6. CONSOLIDADO DE BRECHAS.

Análisis de Brechas

En el presente capítulo se desarrolla lo siguiente:

a. Se toman las brechas identificadas por componente de Gobierno digital
b. Se establecen posibles soluciones.
c. Se determinan las entregas de valor.
d. Se identifican los interesados claves.

7. HOJA DE RUTA.

Se presenta la hoja de ruta elaborada a partir de brechas agrupadas en paquetes de trabajo que generan la misma capacidad a la Entidad.

ANEXO 01. ANALISIS Y PRIORIZACIÓN DE INICITIVAS

Teniendo en cuenta el resultado anterior, se identifican las iniciativas de seguridad y privacidad de la información, los cuales están alineados con el Plan Estratégico de la Entidad, y las necesidades que se identificaron en las coordinaciones como apoyo conforme al resultado del diagnóstico realizado con respecto al cumplimiento y nivel de madurez del modelo de seguridad y privacidad de la información.

Las iniciativas están enmarcadas dentro de los controles sugeridos para garantizar una adecuada arquitectura de seguridad y privacidad de la información y un esquema de defensa a profundidad utilizando soluciones de tecnología y las nuevas tendencias de seguridad de la información.

INCIATIVA	DECRIPCIÓN INICITIVA	ESTRATEGIA SEGURIDAD DE LA INFORMACIÓN OBJETIVOS DE SEGURIDAD			
		GOBIERNO MSPI	GESTIÓN DE RIEGOS DE SEGURIDAD	DESARROLLO Y GESTIÓN DEL PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
I.01	Elaborar e implementar plan estratégico de seguridad y privacidad de la información	**X**			
I.02	Gestionar el sistema de Gestión Seguridad de la información de acuerdo con alcance	**X**			
I.03	Diseñar e implementar programa anual de sensibilización y socialización en seguridad y privacidad de la información	**X**			
INCIATIVA	**DECRIPCIÓN INICITIVA**	**ESTRATEGIA SEGURIDAD DE LA INFORMACIÓN OBJETIVOS DE SEGURIDAD**			
		GOBIERNO MSPI	**GESTIÓN DE RIEGOS DE SEGURIDAD**	**DESARROLLO Y GESTIÓN DEL PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN**	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**
I.04	Actualización del Diagnóstico de Modelo de Seguridad y privacidad de información			**X**	

I.05	Sistematizar el proceso para reportar y escalar los eventos e incidentes de seguridad				**X**
I.06	Crear las políticas que están en el alcance del MSPI de acuerdo con la aplicabilidad			**X**	
I.07	Proyecto de Inventario de activos de información y gestión de riesgos para 2 procesos de la entidad		**X**		

Tabla 4: Iniciativas/Proyectos en un Plan de Seguridad y privacidad de la Información priorizados para ejecución año 2020

ANEXO 2. DEFINICIÓN DEL PORTAFOLIO DE PROYECTOS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se presentan las iniciativas de seguridad agrupadas por proyectos:

PROYECTO	DESCRIPCIÓN PROYECTO	INICIATIVA	DESCRIPCIÓN INICIATIVA
P0	Gestión del programa	I.01	Elaborar e implementar plan estratégico de seguridad y privacidad de la información
P0	Gestión del programa	I.02	Gestionar el sistema de Gestión Seguridad de la información de acuerdo con alcance
P0	Gestión del programa	I.03	Diseñar e implementar un programa anual de sensibilización y socialización en seguridad y privacidad de la información
P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.04	Actualización del Diagnóstico de Modelo de Seguridad y privacidad de información
P2	Gestión de incidentes de Seguridad de la información	I.05	Sistematizar el proceso para reportar y escalar los eventos e incidentes de seguridad

P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.06	Crear las políticas que están en el alcance del MSPI de acuerdo con la aplicabilidad
P3	Gestión de Riesgos de Seguridad de la información	I.07	Proyecto de Inventario de activos de información y gestión de riesgos para 2 procesos de la entidad

Tabla 5. Portafolio de proyectos de seguridad Digital y de la información

HOJA DE RUTA DE PROYECTOS

PROYECTO	DESCRIPCIÓN PROYECTO	INICIATIVA	DESCRIPCIÓN INICIATIVA	TRIMESTRE 2020			
				1	2	3	4
P0	Gestión del programa	I.01	Elaborar e implementar el plan estratégico de seguridad y privacidad de la información				
P0	Gestión del programa	I.02	Gestionar el sistema de Gestión Seguridad de la información de acuerdo con alcance				
P0	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.04	Actualización del Diagnóstico de Modelo de Seguridad y privacidad de información				
P3	Gestión de Riesgos de Seguridad de la información	I.7	Proyecto de Inventario de activos de información y gestión de riesgos para 2 procesos de la entidad				
P0	Gestión del programa	I.03	Diseñar e implementar programa anual de sensibilización y socialización en seguridad y privacidad de la información				
P1	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.06	Crear las políticas que están en el alcance del MSPI de acuerdo con la aplicabilidad				
P2	Gestión de incidentes de Seguridad de la información	I.05	Sistematizar el proceso para reportar y escalar los eventos e incidentes de seguridad				
P3	Gestión de Riesgos de Seguridad de la información	I.07	Proyecto de Inventario de activos de información y gestión de riesgos para 2 procesos de la entidad				

Tabla 6: Hoja de ruta proyectos 2020 Seguridad de la información