CORPORACIÓN AUTÓNOMA REGIONAL DE BOYACÁ

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Corpoboyacá

Región estratégica para la sostenibilidad

SOPORTE TECNOLÓGICO
SUBDIRECCIÓN DE PLANEACIÓN Y SISTEMAS DE INFORMACIÓN
CORPOBOYACÁ
2023

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Corporación Autónoma Regional de Boyacá, Corpoboyacá, creada por la Ley 99 del 22 de diciembre de 1993, lidera el desarrollo sostenible a través del ejercicio de autoridad ambiental, la administración y protección de los recursos naturales renovables, el ambiente y la formación de cultura ambiental, de manera planificada y participativa.

Corpoboyacá como entidad de carácter público, del orden nacional, cuyo objetivo principal ejecución de las políticas, planes, programas y proyectos sobre medio ambiente y recursos naturales renovables, conforme a las regulaciones, pautas y directrices expedidas por el Ministerio de Medio Ambiente; y entendiendo la importancia de una adecuada gestión de la información, Adopta un Modelo de Seguridad y Privacidad de la Información –MSPI enmarcado de la Política de Gobierno Digital y las necesidades de la Corporación.

La Seguridad de la Información, como principio de la Política de Gobierno Digital, busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado y de los servicios que prestan al ciudadano.

La información tiene la característica de ser uno de los activos más importantes para cualquier organización, debido a que de su tratamiento confidencial depende la rentabilidad y continuidad de su modelo de negocio, por esta razón la seguridad de la información resulta ser un factor crítico para la Corporación.

Mediante la utilización del Modelo de Seguridad y Privacidad para las Entidades del Estado, se busca promover el uso de mejores prácticas de seguridad de la información, aplicar el concepto de Seguridad Digital; dar lineamientos para en la implementación que permita identificar y superar las brechas en seguridad de la información.

El presente plan de Seguridad y Privacidad de la Información, tiene como propósito el cumplimiento de los requisitos y lineamientos, que tienen como objetivo, planear y gestionar adecuadamente la seguridad de la información, la gestión de activos, la gestión de riesgos y la continuidad en la prestación de los servicios ofrecidos por la Entidad.

2. OBJETIVO GENERAL

Establecer un plan de actividades de seguridad y privacidad de la información para la Corporación Autónoma Regional de Boyacá - Corpoboyacá, de acuerdo a la Política del Gobierno Digital del Ministerio de las Tecnologías y Comunicaciones –MinTIC, de manera que permita la implementación de mecanismos para la protección de los activos de información de la entidad.

3. OBJETIVOS ESPECÍFICOS

✓ Identificar, actualizar y proteger los activos de información de CORPOBOYACA, con base en los principios de confidencialidad, integridad y disponibilidad.

✓ Establecer actividades para el fortalecimiento de la seguridad de la información

✓ Concientización interna de las políticas en seguridad de la información.

✓ Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.

4. ALCANCE Y DELIMITACIÓN DEL PLAN

El alcance del plan es mantener y mejorar los niveles de seguridad y privacidad de la información y la protección de los activos de información, de acuerdo al Modelo de Seguridad y Privacidad de la Información propuesto por la Política Nacional de Gobierno Digital y teniendo en cuenta los activos de información de la entidad, los procesos, servicios y objetivos corporativos

5. MARCO LEGAL APLICABLE

- ✓ **Constitución Política de Colombia de 1991,** Articulo 15, consagra que todas las personas tienen el derecho a su intimidad personal y familiar y a su buen nombre. De igual modo, tienen el derecho a conocer, actualizar y a rectificar las informaciones que hayan recogido sobre ellas en los bancos de datos y en los archivos de las entidades públicas y privadas.
- ✓ **Ley 23 de 1982,** Ley de propiedad intelectual y derechos de autor.
- ✓ **Ley 527 de 1999,** Ley 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.

- ✓ **Ley 594 de 2000**, Ley General de Archivos, la presente ley tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado.
- ✓ **Ley 1266 de 2008**, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- ✓ **Ley 1437 de 2011**, Código de procedimiento Administrativo y de lo contencioso administrativo,
- ✓ **Ley Estatutaria 1581 de 2012,** Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentada parcialmente en el decreto 1377 de 2013 y en el capítulo 25 del decreto 1074 de 2015,
- ✓ **Decreto 2578 de 2012,** Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye "El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles" entre otras disposiciones.
- ✓ **Decreto 2609 de 2012,** Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.
- ✓ **Norma técnica colombiana NTC/ISO 27001:2013,** Sistema de seguridad de la Información
- ✓ **Norma ISO 27001,** Sistemas de Gestión de la Seguridad de la Información.
- ✓ **Ley 1712 DE 2014,** Ley de Transparencia y del derecho de acceso a la información pública nacional.
- ✓ **Decreto 1078 de 2015,** Decreto único reglamentario del sector de Tecnologías de la Información, por la cual se establece la estrategia de gobierno en línea y dentro de la cual se establece el componente de seguridad y privacidad de la información.
- ✓ **CONPES 3854 de 2016,** Política Nacional de Seguridad Digital.
- ✓ **Decreto 612 de 2018,** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- ✓ **Decreto 1008 de 2018,** Por el 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. Tiene como principio la seguridad de la información, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.
- ✓ **Decreto 2106 de 2019,** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.

6. TÉRMINOS Y DEFINICIONES

Activo de Información. Recurso tangible e intangible de los sistemas de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Entendiendo por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la entidad.

Análisis del riesgo. Uso sistemático de la información para identificar las fuentes y calcular el riesgo.

Amenaza. Son los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos de información, puede ser de dos tipos: Amenazas internas y Amenazas externas. Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

Control. Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

Diagnóstico. Es el análisis que se realiza para determinar cualquier situación y cuáles son las tendencias. Esta determinación se realiza sobre la base de datos y hechos recogidos y ordenados sistemáticamente, que permiten juzgar mejor qué es lo que está pasando.

Evaluación del riesgo. Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo.

Evaluación de la Amenaza. Es el proceso mediante el cual se determina la probabilidad de ocurrencia y la severidad de un evento en un tiempo específico y en un área determinada. Representa la ocurrencia estimada y la ubicación geográfica de eventos probables.

Evento de seguridad de la información. Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida.

Gestión del riesgo. Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

Información. Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Impacto. Es la consecuencia negativa sobre un activo de la materialización de una amenaza.

Incidente de seguridad de la información. Evento que atenta contra la confidencialidad, integridad o disponibilidad de la información y los recursos tecnológicos. Evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

Lineamiento. Una descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos.

MinTIC: Sigla de Ministerio de Tecnología y de Comunicaciones del Gobierno de Colombia

MSPI. Sigla de Modelo de Seguridad y privacidad de la Información MSPI, dispuesto a aplicar por las entidades del estado en el marco de la Política de Gobierno Digital por MinTIC

Normas ISO 27000. El estándar ISO 27000 apunta a exigir niveles concretos y adecuados de seguridad informática, niveles necesarios para las empresas que compiten a través del comercio electrónico y que por lo tanto tienen que exponer sus infraestructuras de información.

Política. Intención y dirección general expresada formalmente por la Dirección.

Principios de seguridad de la Información:

- ✓ **Confidencialidad.** Es la propiedad de la información, por la que se gestiona que es accesible únicamente a personal autorizado a conocer la información.
- ✓ **Integridad.** Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.
- ✓ **Disponibilidad.** Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

SEGURIDAD DE LA INFORMACIÓN: La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

SGSI: Sistema de Gestión de la Seguridad de la Información, es utilizada para referirse a la gestión de los procesos y mecanismos de control que son utilizados para custodiar y proteger de amenazas la información sensible de las organizaciones. Los SGSI permiten a las organizaciones determinar con objetividad que información requiere ser protegida, por qué debe ser protegida, de qué debe ser protegida y como protegerla mediante la planificación e implantación de políticas, procedimientos y controles que mantengan siempre el riesgo por debajo del nivel asumible por la propia organización.

Tratamiento del riesgo: Proceso de selección e implementación de acciones o medidas para mitigar o reducir el nivel del riesgo. El tratamiento de riesgos consiste en buscar los niveles de riesgos aceptables para la organización.

Vulnerabilidad: Debilidad de un activo que puede ser aprovechada por una amenaza. Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas

7. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE CORPOBOYACÁ

La Corporación Autónoma Regional de Boyacá, Corpoboyacá, velará por mantener los principios de integridad, disponibilidad y confidencialidad de la información, mediante la adopción de políticas y procedimientos institucionales, buenas prácticas en seguridad y manejo de activos de información, realizando una adecuada gestión de los mismos y de los riesgos asociados, así como la concientización interna de las políticas en seguridad de la información orientadas al logro de los objetivos estratégicos.

8. PLAN GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El plan de seguridad y privacidad de la información es un documento que denota el compromiso de Corpoboyacá con la seguridad de la información. Este plan contribuye a minimizar los riesgos asociados a con seguridad de la información.

La Corporación Autónoma Regional de Boyacá, velará por la protección de los activos de información, bajo los principios de confidencialidad, integridad, disponibilidad de la información; mediante el diagnóstico, planeación, implementación, gestión y mejora continua dentro de un Modelo de Seguridad y Privacidad de la Información, minimizando de los riesgos asociados a la información, procurando la concientización interna de las políticas en seguridad de la información basada en la Política Nacional de Gobierno Digital.

La eficiencia de la política de seguridad de la información se construye a través del liderazgo y compromiso de la Dirección y la participación activa de los funcionarios, contratistas y terceros, quienes mancomunadamente deberán alcanzar el nivel de cumplimiento de los lineamientos, políticas y requisitos de seguridad de la información, así como el desarrollo de estrategias de mejora continua y gestión oportuna frente a incidentes o eventos de seguridad de la información.

9. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

La seguridad y privacidad de la información, como elemento de la política de gobierno digital, busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos, a través de un Modelo de Seguridad y Privacidad de la Información, denominado también MSPI por sus siglas.

El modelo de seguridad y privacidad de la información – MSPI, contempla un ciclo de operación de cinco (5) fases, las cuales permiten gestionar adecuadamente la seguridad y privacidad de sus activos de información.

En el Modelo de Seguridad y Privacidad de la Información – MSPI, se contemplan 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.

Para la implementación del Modelo de seguridad y privacidad de la Información - MSPI, se identifican 5 fases que orientan el ejercicio para los propósitos de protección de la información de la Entidad, bajo un modelo sostenible, propuesto por el MinTIC y ajustado para Corpoboyacá.

Las fases del ciclo de operación se definen de la siguiente manera basadas en una fase inicial de diagnóstico:

1. Diagnosticar
2. Planear
3. Implementación
4. Gestión
5. Mejora continua

Figura 1 – Ciclo de Operación de seguridad y privacidad de la Información
Fuente: Modelo de Seguridad y Privacidad de la Información - MinTIC

8.1. ACTIVIDADES DEL PLAN SEGURIDAD Y PRIVACIDAD

ACTIVIDADES DEL PLAN SEGURIDAD Y PRIVACIDAD		
ACTIVIDADES / RESULTADOS		**PERIODO**
Realizar o actualizar el Plan de Seguridad de la Información – PSI	-Documento Plan de Seguridad de la Información – PSI.	Primer semestre de 2023
Realizar o actualizar el Plan de tratamiento de riesgos – PTRI	-Documento Plan de Tratamiento del Riesgo de la Información – PTRI.	Primer semestre de 2023
Actualización del nivel de madurez de seguridad y privacidad de la información en la Entidad.	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Primer semestre de 2023
Identificación de vulnerabilidades técnicas y administrativas	Documento de vulnerabilidades técnicas y administrativas (Documento interno - no se publica)	Primer semestre de 2023
Actualización del Inventario de activos de información.	Matriz con la identificación, valoración y clasificación de activos de información.	Primer semestre de 2023
Actualización del Inventario de activos de información.	Matriz con la identificación, valoración y clasificación de activos de información.	Primer semestre de 2023
Política de Seguridad y Privacidad de la Información.	Documento con la política de seguridad de la información, debidamente aprobadas, para posteriormente ser socializadas al interior de la Entidad.	Primer semestre de 2023
Fortalecer la cultura de seguridad de la información en los funcionarios de la entidad.	Dar a conocer las políticas de seguridad a través del curso de Inducción o reinducción o a través de otros medios informativos.	Segundo semestre 2023
Identificación, valoración y tratamiento de riesgo.	Matriz de riesgos con la identificación, análisis y valoración de riesgos de información, de los activos críticos de la entidad	Segundo semestre 2023
Roles y responsabilidades de seguridad y privacidad de la información.	Documento con los roles y responsabilidades de seguridad y privacidad de la información que incluya quien o quienes serán los encargados de seguridad de la información dentro de la entidad.	Segundo semestre 2023

Documentos de Integración del MSPI con el Sistema de Gestión documental.	Documentos relacionados o que resulte de la Integración del MSPI	Segundo semestre 2023
Registro de bases de datos en el RNBD.	Documento relacionado con el Registro o actualización de bases de datos en el RNBD.	Segundo semestre 2023
Plan de sensibilización y comunicación en Seguridad de la Información.	Documento con el plan de sensibilización o capacitación en Seguridad de la Información para funcionarios de la entidad.	Segundo semestre 2023
Transición de IPv4 a IPv6	Documentos con el Plan de diagnóstico de la transición de IPv4 a IPv6 y demás documentos correspondientes a sus fases.	Segundo semestre 2023
Plan de Transición de IPv4 a IPv6	-Documento con las estrategias del plan de implementación y avance de IPv6 en la entidad.	Segundo semestre 2023

10. CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS
30/07/2018	0	Documento inicial
20/01/2020	1	Estructuración de plan de seguridad y privacidad de la información
20/01/2021	2	Estructuración de plan de seguridad y privacidad de la información.
20/01/2022	3	Estructuración de plan de seguridad y privacidad de la información, con ajuste en los objetivos y plan de actividades.
16/01/2023	4	Estructuración de plan de seguridad y privacidad de la información, con ajuste en actividades del plan seguridad y privacidad.