

	CORPORACIÓN AUTÓNOMA REGIONAL DE BOYACÁ	PLANEACIÓN ORGANIZACIONAL	
	SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD	MANUAL	
		MST-01	Página 1 de 25
		VERSIÓN 0	09/02/2023
<b>MANUAL DE POLÍTICAS DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN</b>			



Corpoboyacá

# MANUAL DE POLÍTICAS DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE:	Alfredo Orjuela Peña / Pedro Vela Mendieta	German Gustavo Rodríguez C.	Luis Hair Dueñas Gómez
CARGO / ROL:	Prof. Universitario/ Prof Especializado Soporte Tecnológico	Profesional Especializado Planeación Organizacional	Responsable proceso
FIRMA:	<b>ORIGINAL FIRMADO</b>	<b>ORIGINAL FIRMADO</b>	<b>ORIGINAL FIRMADO</b>

## CONTENIDO

<b>1.</b>	<b>INTRODUCCIÓN .....</b>	<b>3</b>
<b>2.</b>	<b>OBJETIVO.....</b>	<b>4</b>
<b>2.1</b>	<b>OBJETIVOS ESPECÍFICOS.....</b>	<b>4</b>
<b>3.</b>	<b>ALCANCE.....</b>	<b>4</b>
<b>4.</b>	<b>REFERENCIAS NORMATIVAS .....</b>	<b>4</b>
<b>5.</b>	<b>POLÍTICAS DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN .....</b>	<b>6</b>
<b>5.1</b>	<b>POLÍTICA GENERAL DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN DE CORPOBOYACÁ .....</b>	<b>6</b>
<b>5.2</b>	<b>POLÍTICAS ESPECIFICAS PARA LA SEGURIDAD DIGITAL Y DE LA INFORMACIÓN DE CORPOBOYACÁ .....</b>	<b>6</b>
5.2.1	POLÍTICAS DE LA ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN.....	7
5.2.2	POLÍTICAS DE LA ESTRUCTURA ORGANIZACIONAL INTERNA DE SEGURIDAD DE LA INFORMACIÓN .....	7
5.2.3	POLITICAS DE DISPOSITIVOS MÓVILES.....	8
5.2.4	POLÍTICAS DE SEGURIDAD PARA LOS RECURSOS HUMANOS .....	9
5.2.5	POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN .....	11
5.2.6	POLITICAS DE CONTROL DE ACCESO .....	13
5.2.7	POLITICA DE CIFRADO - CONTROLES CRIPTOGRÁFICOS.....	15
5.2.8	POLITICAS DE SEGURIDAD FÍSICA.....	15
5.2.9	POLITICAS DE SEGURIDAD DE LAS OPERACIONES DE TIC.....	17
5.2.10	POLÍTICAS DE SEGURIDAD DE LAS TELECOMUNICACIONES.....	19
5.2.11	POLITICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN ...	20
<b>6.</b>	<b>TÉRMINOS Y DEFINICIONES.....</b>	<b>21</b>
<b>7.</b>	<b>CAMBIOS EFECTUADOS.....</b>	<b>25</b>

COPIA NO CONTROLADA

## 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 y 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, adoptó el Modelo de Seguridad y Privacidad de la Información (MSPI) en el documento Plan de Seguridad y Privacidad de la Información, de acuerdo con la Política de Gobierno Digital y a 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.

El manual de Seguridad de la Información de Corpoboyacá, es un documento que contiene los objetivos, alcance, definiciones, lineamientos, que orientan y apoyan la gestión de seguridad de la información.

**Las políticas de seguridad digital y de la información de Corpoboyacá**, buscan mantener la integridad, confidencialidad y la disponibilidad de la información, proporcionando los lineamientos para la protección y resguardo de los activos de información de la entidad, y minimizando el riesgo asociado.

## 2. OBJETIVO

Establecer las **políticas de seguridad digital y de la información** de la Corporación Autónoma Regional de Boyacá – Corpoboyacá de tal forma que contribuyan al logro de los objetivos institucionales preservando los principios de integridad, disponibilidad y confidencialidad de los activos de información.

### 2.1 OBJETIVOS ESPECÍFICOS

- Instituir las políticas de seguridad digital y de la información de Corpoboyacá, a fin de proteger y resguardar los activos de la información en la entidad.
- Preservar la integridad, disponibilidad y confidencialidad de los activos de información, mediante la adopción de buenas prácticas y la aplicación de políticas y lineamientos que permitan la gestión de riesgos asociados a los mismos.
- Establecer las medidas y controles de seguridad digital y de la información a fin de concientizar a las partes interesadas de la corporación, frente a los riesgos asociados a los activos de información.

## 3. ALCANCE

Las políticas de seguridad digital y de la información establecidas, deben ser conocidas y aplicadas por todos los funcionarios, contratistas, pasantes, administradores de plataformas, proveedores de servicios informáticos y demás partes interesadas que hagan uso de la plataforma tecnológica e informática de la Corporación Autónoma Regional de Boyacá- Corpoboyacá.

## 4. REFERENCIAS NORMATIVAS

A continuación, se listan las normas del marco legal colombiano referente a la seguridad digital y de la información:

- **Constitución Política de Colombia de 1991**, Artículo 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.
- **CONPES 3995 de 2020**: Política Nacional de Confianza y Ciberseguridad.
- **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.
- **Resolución 1519 de 2020**. 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

## 5. POLÍTICAS DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN

La política general de seguridad digital y de la información de la Corporación Autónoma Regional de Boyacá, así como sus lineamientos específicos deben ser conocidos y aplicados por todos los funcionarios, contratistas, pasantes, administradores de plataformas, proveedores de servicio y demás partes interesadas que hagan uso de la plataforma tecnológica y los servicios tecnológicos de la Corporación.

### 5.1 POLÍTICA GENERAL DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN DE CORPOBOYACÁ

La Corporación Autónoma Regional de Boyacá, Corpoboyacá, velará por preservar la integridad, disponibilidad y confidencialidad de los activos de información de tal forma que contribuyan al logro de los objetivos institucionales, mediante la adopción de buenas prácticas, estableciendo lineamientos, controles y concientizando a las partes interesadas en la gestión de riesgos asociados a los mismos.

**Propósitos:** Establecer las políticas de seguridad digital y de la información de la Corporación Autónoma Regional de Boyacá – Corpoboyacá de tal forma que contribuyan al logro de los objetivos institucionales preservando los principios de integridad, disponibilidad y confidencialidad de los activos de información.

- Instituir las políticas de seguridad digital y de la información de Corpoboyacá, a fin de proteger y resguardar los activos de la información en la entidad.
- Preservar la integridad, disponibilidad y confidencialidad de los activos de información, mediante la adopción de buenas prácticas y la aplicación de políticas y lineamientos que permitan la gestión de riesgos asociados a los mismos.
- Establecer las medidas y controles de seguridad digital y de la información a fin de concientizar a las partes interesadas de la corporación, frente a los riesgos asociados a los activos de información.

### 5.2 POLÍTICAS ESPECIFICAS PARA LA SEGURIDAD DIGITAL Y DE LA INFORMACIÓN DE CORPOBOYACÁ

A continuación, se relacionan el marco general de las políticas de seguridad de la Información:

1. Políticas de estructura organizacional interna de seguridad de la información
2. Políticas de seguridad para los recursos humanos
3. Políticas de gestión de activos de Información y uso aceptable de activos
4. Políticas de control de acceso
5. Políticas de cifrado - controles criptográficos
6. Políticas de seguridad física
7. Políticas de seguridad de las operaciones de TIC
8. Políticas de seguridad de las telecomunicaciones
9. Políticas de adquisición, desarrollo y mantenimiento de sistemas de información

### **5.2.1 POLÍTICAS DE LA ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN**

A continuación, se presentan las políticas de estructura organización interna de seguridad de la información y políticas de dispositivos móviles, con el propósito de establecer un marco de referencia de gestión y operación de seguridad en la entidad:

- Políticas de estructura organización interna de seguridad de la información
- Políticas de dispositivos móviles

### **5.2.2 POLÍTICAS DE LA ESTRUCTURA ORGANIZACIONAL INTERNA DE SEGURIDAD DE LA INFORMACIÓN**

A continuación, se presentan las políticas de la estructura de la organización interna de seguridad de la información, con el propósito de establecer un marco de referencia de gestión y operación de seguridad de la información en la entidad:

- La Corporación Autónoma Regional de Boyacá - Corpoboyacá, adoptó el Modelo de Seguridad y Privacidad de la Información (MSPI) en el documento Plan de Seguridad y Privacidad de la Información, de acuerdo con la Política de Gobierno Digital y a las necesidades de la Corporación.
- Es responsabilidad de los funcionarios, contratistas, pasantes y demás personal de apoyo de Corpoboyacá, velar por el cuidado de los activos de información que manejan o que estén a su cargo y de cumplir los lineamientos en seguridad de la información dados por la Corporación.
- Los funcionarios, contratistas, pasantes y demás personal de apoyo de Corpoboyacá, NO deben suministrar información clasificada y/o reservada o información con datos personales tratados por la Corporación o cualquier otra información que resulte crítica para la entidad por cualquier medio a ninguna entidad externa sin la previa autorización del Director, Subdirector respectivo o jefe de la dependencia.
- Todo funcionario, contratista, pasante y demás personal de apoyo que por algún motivo utilice la plataforma tecnológica y los servicios tecnológicos disponibles, tiene la responsabilidad de velar por la integridad, disponibilidad y confidencialidad de la información que trate o maneje de su área o proceso, especialmente si dicha información está protegida por reserva legal o ha sido calificada como clasificada, confidencial o que contenga datos personales tratados por la Corporación y/o que resulte crítica para la entidad.
- Los funcionarios, contratistas, pasantes y demás personal de apoyo de Corpoboyacá son responsables de la información que manejan y deberán cumplir los lineamientos de seguridad de la información dados por la Corporación, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

- Los contratistas deben solicitar el visto bueno al proceso Gestión Soporte Tecnológico en el formato respectivo de exclusión de obligaciones de acuerdo al procedimiento emitido por Gestión Humana, una vez terminado el contrato o su vinculación laboral con la entidad.
- El Proceso de Soporte Tecnológico o de seguridad de la información debe mantener una lista de contactos con autoridades u organismos como: Policía Nacional, Bomberos, Defensa Civil, Guardas y/o Líderes de Seguridad física de la entidad, para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad de la información y se requieran.
- El Proceso de Soporte Tecnológico o de seguridad de la información deben mantener contacto y generar mecanismos de articulación con grupos de interés en seguridad de la Información, tales como foros, seminarios, cursos, conferencia en línea, entre otros mecanismos de información, con el fin de recibir, compartir o intercambiar conocimientos y buenas prácticas en seguridad de la información.
- Las Subdirecciones, áreas y procesos de la Corporación, deberán incluir en sus proyectos, la gestión de seguridad de la información, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto.

### 5.2.3 POLÍTICAS DE DISPOSITIVOS MÓVILES

A continuación, se presentan políticas de dispositivos móviles que gestionen información de la entidad, con el propósito de establecer un marco de referencia para la operación de estos dispositivos:

- Todos los dispositivos móviles como celulares, tabletas o portátiles de la Corporación que almacenen información de la entidad deben contar con un medio de autenticación, como un patrón, código o cualquier otro mecanismo de seguridad para el acceso y/o desbloqueo.
- Los funcionarios, contratistas, pasantes y demás personal de apoyo que operen dispositivos móviles de propiedad de la Corporación y con debida autorización, deberán hacer periódicamente copias de respaldo y permitir actualización del sistema operativo, antivirus y demás aplicaciones que requieran.
- El acceso a internet desde dispositivos móviles personales de funcionarios, visitantes, contratistas y demás personal de apoyo, se podrá otorgar mediante red inalámbrica (Wi-Fi), cuando existan las condiciones técnicas y siempre que la comunicación se dé por red diferente a la red interna de datos, de manera que se minimice el riesgo de acceso no autorizado a través de la red. El Proceso de Soporte Tecnológico gestionará o administrará estas conexiones.
- Los funcionarios, contratistas, pasantes y demás personal de apoyo son responsables de hacer buen uso de los dispositivos móviles que procesan información de la Corporación, conectándolos a redes seguras y NO conectar los dispositivos a sitios públicos que ofrecen acceso a internet por WIFI, esto con el fin de evitar acceso no autorizado o divulgación de la información almacenada o procesada por estos.

- Los funcionarios, contratistas, pasantes y demás personal de apoyo que conecte medios extraíbles, dispositivos móviles, memorias USB, entre otros dispositivos a los equipos de la Corporación, deberán hacer buen uso de los mismos y no deberán extraer información, salvo los casos justificados y autorizados por el Director, Subdirector, jefes de Oficina o Líderes del proceso.
- Los funcionarios, contratistas, pasantes y demás personal de apoyo son responsables de hacer buen uso de los dispositivos móviles que procesan información de la Corporación, conectándolos a redes seguras y de NO conectarlos a sitios públicos que ofrecen acceso a internet por WIFI, esto con el fin de evitar acceso no autorizado o divulgación de la información almacenada o procesada por estos.
- Para la modalidad de Teletrabajo o de trabajo en casa, el proceso de Soporte tecnológico proveerá los mecanismos seguros de conexión remota hacia y desde la red LAN de Corpoboyacá, como VPN y otros mecanismos de conexión segura.
- Los funcionarios, contratistas, pasantes y demás personal de apoyo que estén en modalidad de teletrabajo o trabajo en casa deberán mantener conexión a internet con frecuencia para mantener los sistemas operativos y demás aplicaciones actualizadas.
- Los funcionarios, contratistas, pasantes y demás personal de apoyo que estén en modalidad de teletrabajo o trabajo en casa NO deben hacer divulgación de información considerada como clasificada, o reservada, confidencial o de datos personales sin la debida autorización y que puedan poner en riesgo la seguridad de la información de la Corporación.
- Los funcionarios y demás personal de apoyo que estén en modalidad de teletrabajo o trabajo en casa y que hagan uso de equipos de la Corporación, deberán aplicar las políticas institucionales de cuidado y conservación de los equipos que estén bajo su responsabilidad y de realizar copias de seguridad de manera periódica.

#### **5.2.4 POLÍTICAS DE SEGURIDAD PARA LOS RECURSOS HUMANOS**

A continuación, se presentan las políticas con el propósito de establecer lineamientos de verificación y validación de documentos y otros requisitos legales para el personal de funcionarios antes, durante y después de asumir el empleo en la Entidad o para el caso de los contratistas de prestación de servicios (CPS) antes, durante y después del contrato.

#### **POLÍTICAS ANTES DE ASUMIR EL EMPLEO POR PARTE DE SERVIDORES PÚBLICOS O PERSONAL DE PRESTACION DE SERVICIOS.**

- El proceso de Gestión Humana, deberá establecer y/o mantener los procedimientos según correspondan para la selección y vinculación de funcionarios (Personal de planta) a la entidad, los cuales se incluirán en una lista que contenga los aspectos necesarios de verificación y revisión de los antecedentes del personal antes de la vinculación a la Entidad, de acuerdo a lo exigido por la Corporación y a lo reglamentado por ley.
- El proceso de Contratación, deberá establecer, mantener y verificar previo al contrato una lista de chequeo que contenga los aspectos necesarios para la revisión de los antecedentes del personal a contratar por prestación de servicios de acuerdo a lo exigido por la Corporación y a lo

reglamentado por ley, de tal forma q aporten a conservar los principios de seguridad de la información.

- Los procesos de vinculación de servidores públicos y contratación de prestación de servicios (CPS) deben incluir una autorización para el tratamiento de los datos personales de funcionarios o contratistas de prestación de servicios, de acuerdo con la Política de tratamiento de datos de acuerdo a lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios. Esta autorización podrá quedar de manera explícita en un documento para el caso de funcionarios o en la minuta del contrato para contratistas.
- Todo servidor público o contratista debe suscribir con la Entidad, un documento de acuerdo de confidencialidad y no divulgación de la información considerada clasificada y/o reservada o confidencial, o que contenga datos personales tratados por la Corporación. Solo se podrá divulgar en los casos autorizados por la Entidad. El acuerdo de confidencialidad podrá quedar de manera explícita en un documento para el caso de funcionarios o en minuta del contrato para contratistas.

### **POLÍTICAS DURANTE EL EMPLEO O CONTRATO.**

- Los funcionarios públicos, contratistas, pasantes y personal de apoyo de Corpoboyacá son responsables de la información que manejan y deben velar por la seguridad de la misma cumpliendo los lineamientos o políticas de seguridad de la información dados por la Corporación.
- Una vez formalizado el proceso de vinculación a la Corporación, el funcionario podrá solicitar la apertura de cuentas de usuario que requiera mediante el formato de Administración Cuentas de Usuario, autorizado por el Director o Subdirector respectivo y enviar la solicitud al proceso de Soporte Tecnológico.
- El Proceso de Gestión Humana deberá establecer en los planes de capacitación o en jornadas de inducción o reinducción temas relacionados con la SEGURIDAD DIGITAL Y DE LA INFORMACIÓN.
- El Proceso de Soporte Tecnológico, dará a conocer los lineamientos o políticas de la SEGURIDAD DIGITAL Y DE LA INFORMACIÓN. Estos lineamientos o políticas se podrán incluir o dar a conocer en las jornadas de inducción y reinducción o en otros espacios o medios que consideren. El Proceso de Soporte Tecnológico, puede dar a conocer también las políticas o lineamientos en materia de SEGURIDAD DIGITAL Y DE LA INFORMACIÓN a través de medios comunicación digital como el correo electrónico, afiches, videos, videoconferencias, página web, entre otros.

### **POLITICAS DE TERMINACIÓN O CAMBIO DE RESPONSABILIDADES EN EL EMPLEO.**

- Después que los funcionarios, contratistas o pasantes dejan de prestar los servicios o terminen su vinculación con Corpoboyacá, deben entregar la información generada a raíz de su labor al Supervisor, Coordinador o Jefe inmediato según corresponda. Una vez retirado el funcionario o contratista debe comprometerse a NO utilizar, comercializar o divulgar los productos o la información generada o conocida durante labor en la Corporación y en especial la relacionada con la información clasificada, confidencial y reservada o que contenga datos personales recogidos durante su labor en la entidad.

- El funcionario debe entregar los activos de información de acuerdo a los procedimientos de terminación o cambio de empleo.
- El jefe inmediato o funcionario(s) encargado(s) debe custodiar los activos de información de la Corporación, que se encuentra bajo responsabilidad de un funcionario, cuando existe una novedad de retiro temporal o definitivo, suspensión, vacaciones o cambio de funciones o cargo.
- El supervisor del contrato o a quien se delegue debe custodiar la información de la Corporación bajo la responsabilidad de un contratista en caso de terminación anticipada, definitiva, temporal o cesión del contrato.
- Una vez formalizado la desvinculación de un funcionario, pasante o contratista (si aplica), éste debe solicitar la autorización del cierre de cuentas del usuario mediante el formato de administración de cuentas de usuario al subdirector respectivo o supervisor y enviarlo al proceso de Soporte Tecnológico.
- El proceso de Gestión Humana y el funcionario que se desvincule de la Corporación, deberán informar la novedad de retiro mediante el formato de administración de cuentas de usuario al Proceso de Soporte Tecnológico a fin de realizar inactivar las credenciales de acceso a los sistemas de información.
- Nota: Es responsabilidad del funcionario realizar la copia de seguridad del correo electrónico asignado y de la información a su cargo antes de la desvinculación.
- Los funcionarios, contratistas o pasantes que terminen su vinculación con la Corporación, deben entregar al proceso de Gestión Humana el carnet o cualquier elemento de autenticación o prenda de vestir que lo distinga o acredita como funcionario o contratista de Corpoboyacá.

## 5.2.5 POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

**Propósito:** Establecer lineamientos para la identificación y valoración de los activos de información de la Entidad, y definir las responsabilidades para su protección y uso aceptable de activos.

### **POLÍTICAS DE RESPONSABILIDAD SOBRE LOS ACTIVOS Y USO ACEPTABLE DE ACTIVOS**

- El Proceso de Soporte Tecnológico se encargará de mantener el formato de registro de activos de Tecnologías de la información –TI de Corpoboyacá.
- Los funcionarios, contratistas, pasantes o personal de apoyo en cada proceso son los responsables de custodiar los activos de información a su cargo, tales como: equipos de cómputo, portátiles, servidores, redes de datos, entre otros y las aplicaciones o sistemas de información, propios de cada proceso o área de manera que se propenda por la seguridad de la información de estos activos.
- Los funcionarios, pasantes o personal de apoyo que hayan recibido aprobación para tener acceso a sistemas de Información, servicios de Internet, estaciones de trabajo corporativas o computadoras portátiles, entre otros recursos informáticos, deberán aplicar los lineamientos y políticas de en seguridad digital y de la información establecidas.

- Los funcionarios, pasantes o personal de apoyo que hagan uso del servicio de correo electrónico, Internet, equipos de cómputo, dispositivos móviles, portátiles, entre otros equipos y servicios informáticos de Corpoboyacá, deben usarlos únicamente para el ejercicio de las funciones o actividades contratadas.
- Se prohíbe la consulta, exhibición, visualización, circulación y/o almacenamiento de material pornográfico, material obsceno, discriminatorio u ofensivo que atente contra la dignidad de las personas usando los recursos o servicios informáticos de Corpoboyacá.
- Se prohíbe, la transmisión, reproducción, circulación y/o almacenamiento de materiales que violen la regulación colombiana frente a los derechos de autor o propiedad intelectual.
- Se prohíbe el envío o reenvío de mensajes que sean considerado como Correo no deseado (Spam).
- Los funcionarios, pasantes o personal de apoyo deben hacer entrega de los activos bajo su responsabilidad de acuerdo a los procedimientos establecidos por la Corporación para la desvinculación o finalización del contrato.
- Los contratistas o terceros que reciban, generen, procesen o administren información, a causa o con relación del contrato, deben hacer buen uso de los misma y NO realizar divulgación de información sin la debida autorización de los funcionarios líderes, supervisor, jefe de oficina territorial o del subdirector respectivo.

## **POLÍTICAS DE CLASIFICACIÓN DE LA INFORMACIÓN.**

**Propósito:** Establecer lineamientos para la protección y organización de la información de la Entidad.

- El proceso de Soporte Tecnológico debe realizar las acciones correspondientes para el registro y actualización de activos de información, así como para la información clasificada y/o reservada.
- El proceso de Gestión Documental debe mantener actualizadas las Tablas de Retención Documental (TRD) con la clasificación de las series, Subseries y documentos en ella contenidas y demás instrumentos archivísticos, de acuerdo a la normatividad del Archivo General de la Nación - AGN, como instrumentos de apoyo para la gestión, clasificación y registro de los activos de información de la Entidad.
- El proceso de Gestión Documental debe mantener el Cuadro de clasificación documental.
- El proceso de Gestión Documental debe mantener el Inventario documental
- Los funcionarios, pasantes o personal de apoyo deben aplicar la Tabla de Retención Documental TRD para clasificar la información en cada proceso o área
- Los funcionarios, pasantes o personal de apoyo deben tener en cuenta la condición de la información de clasificación y/o de reserva de la Información y de protección de datos personales para el envío de información a entidades externas.

- La Subdirección Administrativa y Financiera de la entidad debe mantener un procedimiento o guía para el rotulado de los activos físicos de toda la entidad.

## **POLÍTICAS DE MANEJO DE LOS SOPORTES REMOVIBLES Y DE ALMACENAMIENTO.**

**Propósito:** Establecer lineamientos para la gestión de medios removibles y de almacenamiento.

- Todo medio removible debe ser escaneado mediante el antivirus suministrado por la entidad cada vez que se conecte a un equipo.
- Es responsabilidad de los funcionarios, pasantes o personal de apoyo tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío del mismo.
- El Proceso de Soporte Tecnológico deberá emplear técnicas o herramientas de borrado seguro de información en los medios de almacenamiento como los disco duros internos o externos que serán objeto de reutilización, de cambio o dados para baja, con el fin de controlar el uso no autorizado de la información contenida en estos medios.
- Los equipos de cómputo, servidores, portátiles ente otros elementos informáticos que requieran ser trasladados de sede, deben ser embalados haciendo uso de las mejores prácticas a fin de velar por su conservación

### **5.2.6 POLITICAS DE CONTROL DE ACCESO**

**Propósito:** Regular el acceso a los sistemas de información, las instalaciones de procesamiento de información y otros lineamientos de control de acceso.

#### **POLITICAS DE CONTROL DE ACCESO.**

- Los funcionarios, pasantes o personal de apoyo tendrán acceso sólo a la información necesaria para el desarrollo de sus actividades. En este sentido los procesos internos o terceros que administren plataformas tecnológicas de la Corporación concederán privilegios en los equipos, sistemas de información y demás plataformas tecnológicas, basados en el principio del menor privilegio. Para otorgar el acceso es requerida la autorización explícita mediante el formato respectivo.
- Los funcionarios, pasantes o personal de apoyo que requieran acceso a los sistemas de información, servicios y/o recursos tecnológicos dispuestos por Corpoboyacá, solicitará autorización al proceso de Soporte Tecnológico, mediante el formato respectivo para la creación de cuentas y acceso a los sistemas de información. Este formato debe estar autorizado por el Director, Subdirector, Secretario General o el Jefe de Oficina Territorial, según pertenezca el usuario que realiza la solicitud. Para el caso de los Contratistas la creación de cuentas debe ser autorizado por el Supervisor del contrato.
- Otros usuarios terceros que requiera acceso a los recursos y/o plataformas de tecnologías de información de la Corporación, tendrán acceso estrictamente a los recursos necesario para el

cumplimiento de su labor, accesos que deben ser aprobados por el Jefe inmediato, supervisor o coordinador.

- La conexión entre sistemas de información de la entidad y otros sistemas o aplicativos de terceros debe ser avalada por el Proceso Gestión Soporte Tecnológico con el fin conservar la seguridad digital y de la información de la Corporación.
- Todos los privilegios para el uso y acceso de los sistemas de información de la Entidad deben terminar o inactivarse inmediatamente después de que el funcionario o colaborador termina de prestar sus servicios a la Entidad.
- Los funcionarios, pasantes o personal de apoyo que utilicen las plataformas tecnológicas o los servicios tecnológicos disponibles, tiene la responsabilidad de velar por la integridad, confidencialidad y disponibilidad de la información que maneje, especialmente si está protegida por reserva legal o ha sido clasificada como confidencial o crítica.
- El acceso a los sistemas de información de la entidad debe realizarse por medio de códigos de identificación y palabras claves (contraseñas únicas) para cada usuario o por métodos de identificación única segura.
- El acceso de los usuarios y equipos a la red de datos de la Corporación, se hace a través de mecanismos de autenticación de usuario y clave en la red de la Corporación (Directorio Activo), el cual debe estar previamente autorizado lo que permitirá el ingreso del usuario al equipo, a las aplicaciones y recursos o servicios de la red.
- Los computadores portátiles de propiedad de los colaboradores podrán ser conectados a la red interna para proporcionar conexión a internet, con previa autorización del Director, Subdirector, funcionario líder o del proceso de Soporte Tecnológico, sin que sean registrados en el servidor de dominio de la red LAN (directorío activo) de Corpoboyacá, teniendo en cuenta que al registrar estos equipos se aplicarán políticas y restricciones internas.
- Los usuarios no deben almacenar en los discos duros de los computadores, discos externos o discos virtuales de red, archivos de vídeo, música, fotos y/o cualquier tipo de archivo con información personal que no sean de carácter institucional o laboral.
- Los funcionarios, pasantes o personal de apoyo deberán hacer buen uso de las páginas de redes sociales como Facebook, YouTube, entre otras. Estas conexiones podrán ser monitoreadas y/o restringidas por el personal de Soporte Tecnológico.
- La creación de cuentas de usuarios de equipo o dominio, de correo electrónico, entre otros sistemas de información, estará a cargo del proceso de Soporte Tecnológico de la entidad o quien se delegue.
- Los usuarios autorizados por el Líder de Soporte Tecnológico, tendrán el privilegio de rol de superusuario (usuario Administrador) según el rol desempeñado, para ejercer administración sobre los sistemas de información a cargo.
- Cualquier cambio en los privilegios, permisos, roles o perfiles de los usuarios en los sistemas de información, deberán ser solicitados al líder del proceso a través del formato de Administración Cuentas Usuario.

- Las credenciales asignadas (usuario y clave) de acceso a los sistemas de información, servidores, equipos y demás servicios informáticos son asignadas de manera individual y cada usuario debe mantenerla de manera confidencial. Las credenciales de acceso son de uso personal e intransferible, por tanto, el usuario es responsable por el acceso, modificación o registro que se haga en las plataformas asignadas con dichas credenciales.
- El proceso de Soporte tecnológico, establecerá el tiempo de vigencia de las credenciales de acceso a los sistemas de información, una vez finalizado el periodo establecido, los usuarios deben realizar el cambio de contraseñas conforme a las indicaciones dadas por el Proceso de Soporte Tecnológico y configuradas en los sistemas de información.

### 5.2.7 POLITICA DE CIFRADO - CONTROLES CRIPTOGRÁFICOS

**Propósito:** Establecer política en el uso de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información de la Entidad.

- Los sistemas de información y aplicativos de conexión deben hacer uso de métodos o mecanismos de cifrado para el acceso a los mismos, como clave cifrada y comunicación cifrada, entre otros para el acceso y transmisión de información de estos sistemas, en especial para la transmisión de información pública reservada o información pública clasificada.
- Se debe propender por el uso de firmas digitales para proporcionar un medio de protección de la autenticidad e integridad de los documentos electrónicos.
- Las conexiones remotas a los equipos de la red de área local deben establecerse a través de una conexión segura como VPN u otros mecanismos de conexión segura (conexión cifrada) y avalados por el proceso de Soporte Tecnológico, la cual pueden ser monitoreadas por este proceso.

### 5.2.8 POLITICAS DE SEGURIDAD FÍSICA

**Propósito:** Establecer lineamientos para prevenir el acceso físico no autorizado, seguridad en las áreas o en las instalaciones de procesamiento de información de la Entidad.

#### POLITICAS DE ÁREAS SEGURAS

- Los puntos de acceso de Corpoboyacá deben ser controlados y monitoreados por el personal servicio de vigilancia y seguridad privada con el fin de minimizar los riesgos de hurtos y acceso no autorizado.
- El personal de vigilancia debe contar con todos los elementos de dotación, identificación, protección y comunicación, ente otros que facilitan el cumplimiento de sus funciones de seguridad.
- El personal de guardia de seguridad debe controlar el ingreso y salida de personas, paquetes y en especial equipos de cómputo, realizando el registro respectivo.
- Los funcionarios, pasantes o personal de apoyo deben acreditarse con las credenciales para el ingreso de la Entidad. De ser establecida documento físico, este debe portarlo en lugar visible durante la permanencia en la institución

- En el ingreso de visitantes a las oficinas administrativas, debe ser controlado, confirmando el ingreso y autorización al área respectiva. El área que recibe la visita, debe de estar atento y vigilar las actividades realizadas por el visitante.
- Las zonas de carga y descarga de mercancía, cajas o paquetes, entre otros, debe ser monitoreado y controlado por el personal de seguridad y vigilancia.
- El personal de seguridad y vigilancia de la Corporación debe realizar monitoreo ininterrumpido a las áreas de accesos, pasillos, zonas de concurrencia entre otros.
- La Subdirección Administrativa y financiera o quien esta delegue es la única autorizada del acceso, custodia del material de grabación del Circuito Cerrado de Televisión –CCTV.
- El personal de seguridad debe orientar a los usuarios visitantes, sobre la ubicación del área a visitar.
- El ingreso de vehículos a parqueaderos, debe ser controlado por el personal de guardia de seguridad de acuerdo a las condiciones, horarios, establecidas por la Corporación.
- El personal de vigilancia debe realizar rondas preventivas brindando seguridad a las instalaciones y a los usuarios.
- Está restringido el acceso al centro de cómputo o infraestructuras TICS, a personal no autorizado. El personal diferente a los funcionarios de Soporte Tecnológico que haya sido autorizado debe estar acompañado por el personal de Corpoboyacá que labora cotidianamente en dichas áreas.

#### POLITICAS DE SEGURIDAD EN EQUIPOS DE COMPUTO.

**Propósito:** Establecer lineamientos para la seguridad de los equipos de cómputo de la Entidad.

- Los Funcionarios públicos, pasantes, contratistas y demás personal de apoyo deben situar los equipos de cómputo e impresoras en áreas adecuadas para reducir el riesgo contra amenazas ambientales, caídas o accesos no autorizado.
- Solo el personal autorizado por el proceso de Soporte Tecnológico puede llevar a cabo el mantenimiento o las reparaciones a los equipos de cómputo, servidores, red de datos o servicios informáticos de la Corporación. El personal de soporte técnico externo a cargo de servicios o infraestructura tecnológica por razones contractuales podrá realizarlo de acuerdo al contrato.
- El proceso de Soporte Tecnológico debe entregar los equipos en reparación o equipos nuevos a usuarios con las siguientes configuraciones establecidas en la lista de chequeo y verificar requerimientos adicionales del rol del usuario.
- Los funcionarios, contratistas, pasantes y demás personal de apoyo de Corpoboyacá, que sospechan de infección por un virus o comportamiento inusual en sus equipos de cómputo, deben realizar el reporte al proceso de Soporte Tecnológico y en lo posible no utilizar la computadora o desconectarla de la red y seguir indicaciones del Proceso de Soporte Tecnológico.

- Las actividades de mantenimiento preventivo de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en los servicios, deberán ser programados.
- Se deben proteger los equipos de cómputo y de comunicaciones con las medidas eléctricas adecuadas necesarias para la operación normal y protección de los mismos.
- Todos los escritorios (mesas de trabajo) deben permanecer organizados y limpios para proteger documentos en papel y dispositivos electrónicos, con fin de reducir los riesgos de acceso no autorizado, pérdida o daño de la información.
- Los funcionarios, pasantes o personal de apoyo de Corpoboyacá durante las ausencias deben guardar en lugar seguro, las carpetas, documentos físicos, medios de almacenamiento, entre otros elementos con el fin de prevenir daños, pérdidas, modificaciones o acceso no autorizados.
- Los funcionarios, pasantes o personal de apoyo de Corpoboyacá, antes de ausentarse de su puesto de trabajo por periodos cortos deben bloquear la pantalla del computador a su cargo, para prevenir modificaciones o acceso no autorizados.
- Se debe utilizar la red regulada de energía (tomas naranjas de canaleta de datos) para conectar equipos de cómputo como la CPU, monitor o Equipo Portátil. NO se deben conectar a esta red las impresoras, plotters, cargadores de celulares, grabadoras, licuadoras, fotocopiadoras, parlantes, secadores de cabello, aires acondicionados, ventiladores, taladros, cámaras fotográficas, de video entre otros que hagan uso de motores, ya que causan ruido eléctrico, sobrecargas eléctricas y daños en los sistemas de UPS y en los equipos de cómputo conectados a la red regulada.
- Soporte Tecnológico es el proceso autorizado a realizar todo cambio de software o hardware que se requiera en los equipos de cómputo y periféricos de Corpoboyacá (Instalación y actualización de programas de software, cambios de procesador, memoria, discos, tarjetas entre otros). También lo puede realizar un tercero autorizado por la corporación con ocasión de contrato.

### 5.2.9 POLÍTICAS DE SEGURIDAD DE LAS OPERACIONES DE TIC

**Propósito:** Establecer lineamientos para las operaciones generales que se realicen sobre las Tecnologías de la Información y Comunicación – TIC

#### POLITICAS DE SEGURIDAD DE LAS OPERACIONES DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN - TIC

- El proceso de Soporte Tecnológico podrá realizar monitoreo a las plataformas relacionadas con tecnologías de información y comunicación de la Entidad que considere a fin de mantener integridad, confiabilidad y disponibilidad de la información.
- El intercambio electrónico de información con sistemas de entidades externas se realizará con base en estándares de documentos electrónicos y mensajes de datos establecidos por Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, que garanticen la integridad, confidencialidad, disponibilidad de la información.
- La Corporación se reserva el derecho de acceder a las cuentas de correo corporativo asignadas por la Entidad en caso de requerirse y cuando el funcionario responsable de la cuenta no se

encuentre presente o disponible en la Entidad por el motivo que fuere. Para la apertura de dichas cuentas se deberá solicitar autorización al Director o Subdirector o jefe inmediato respectivo.

- La propiedad intelectual desarrollada o concebida por funcionarios, contratistas o pasantes durante una labor o actividad con la Corporación, es propiedad exclusiva de Corpoboyacá. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual de productos de actividades o labores contratadas y/o pagadas por la Corporación.
- Los funcionarios, pasantes o personal de apoyo que requieren algún servicio informático como servicio de red de datos, instalación o actualización de software, adquisición de software o hardware, mantenimiento de equipo informático, copias de seguridad, entre otros, deberá solicitarlo al proceso de Soporte Tecnológico a través del formato de solicitud de servicio informático. El servicio informático se realizará solo a equipos y software de propiedad o en comodato con Corpoboyacá.
- El Proceso Gestión Soporte Tecnológico divulgará, las políticas, estándares o procedimientos en materia de seguridad informática.
- Si los usuarios sospechan que hay algún usuario no autorizado intentando acceder a los servicios o recursos informáticos, o haciendo mal uso de los mismos deberá informarlo de manera inmediata al Proceso Soporte Tecnológico.
- Los funcionarios, pasantes o personal de apoyo que realicen actividades de administración de los sistemas de información o servicios tecnológicos de la Corporación son responsables por la implementación de los controles de seguridad definidos en estas políticas de seguridad sobre dichos sistemas o servicios.
- El proceso Gestión Soporte Tecnológico, debe realizar y actualizar periódicamente un plan de contingencia que permita a las aplicaciones críticas, sistemas de Información y comunicación estar disponibles ante una falla o interrupción en los mismos.
- Los sistemas de Información deben propender porque se configure de manera que mantengan la separación física y lógica de los ambientes o entornos de desarrollo, pruebas y producción.
- La Corporación adoptará medidas para publicar la información de acuerdo a la Ley de derecho de acceso a la información pública y demás normas que la regulan, en materia de acceso a la información pública, accesibilidad web, seguridad digital y datos abiertos. Así como medidas aceptables de seguridad digital, para mitigar riesgos de incidentes cibernéticos, atendiendo los lineamientos de gobierno digital en materia de seguridad digital, asegurado las condiciones mínimas técnicas y de seguridad digital en los sitios web y de acuerdo a la normatividad aplicable.

## POLITICAS DE COPIAS DE SEGURIDAD

**Propósito:** Establecer lineamientos de copias de seguridad de los equipos y de los sistemas de información de la entidad.

- Los funcionarios, pasantes, personal de apoyo o terceros que sean administradores de los sistemas de información de Corpoboyacá deben realizar o programar copias periódicas de los sistemas de información a cargo.

- El almacenamiento de copias de seguridad de los sistemas de información deberá mantenerse en un lugar externo o en medio de almacenamiento diferente al sitio dónde se procesa dicha información.
- Los funcionarios, pasantes o personal de apoyo que generen o almacenen información en los equipos de cómputo de la Corporación, serán los responsables de realizar el respaldo de dicha información, siguiendo las indicaciones o procedimiento de Soporte Tecnológico. Los funcionarios, son responsables de realizar las copias de la información que resida en el equipo asignado de acuerdo a los instructivos generados por el proceso de soporte tecnológico.

## POLITICAS DE CONTROL DEL SOFTWARE

**Propósito:** Establecer lineamientos para el control e instalación de software en la Entidad

### GESTIÓN, INSTALACION O ACTUALIZACION DEL SOFTWARE

- Todo software que utilice Corpoboyacá será adquirido de acuerdo con las normas legales vigentes y siguiendo los procedimientos de la Entidad.
- El proceso de Soporte Tecnológico debe controlar la instalación de software en los equipos de la Corporación para los usuarios finales.
- El proceso de Soporte Tecnológico debe mantener un inventario de las licencias de software de Corpoboyacá.
- Se prohíbe descarga e instalación de software NO Licenciado en los equipos de la Corporación, con excepción del software con licencia GNU, similar y/o que se puedan descargar y usar libremente. El proceso de Soporte Tecnológico es el único autorizado para realizar la instalación o desinstalación del software en lo Equipos de la Entidad.
- Los funcionarios, pasantes o personal de apoyo que requieren algún servicio informático como instalación o actualización de software, adquisición de software, deberá solicitarlo al proceso de Soporte Tecnológico a través del formato o mecanismo de solicitud de servicio informático. El proceso de Soporte analizará dicha solicitud evaluará la viabilidad.

## 5.2.10 POLÍTICAS DE SEGURIDAD DE LAS TELECOMUNICACIONES

**Propósito:** Establecer lineamientos para asegurar la protección de la información en las redes de telecomunicaciones de la Entidad.

### GESTIÓN DE LA SEGURIDAD DE LAS REDES

- El proceso de Soporte Tecnológico puede establecer mecanismos de monitoreo sobre las conexiones y servicios en las redes de datos de la Corporación con fines de soporte, monitoreo y de seguridad de la información.

- El proceso de Soporte Tecnológico es el área encargada de la administración de la red interna de datos, la cual debe estar controlada y administrada por un sistema de Directorio Activo (Controlador de Dominio) o una herramienta similar que cumpla con dicha tarea de autenticación y seguridad.
- El Centro de Datos Principal de la Corporación (Datacenter físico), así como sus equipos, servidores conexiones y demás elementos de este lugar, deberán estar resguardados bajo medidas de seguridad adecuadas con mecanismos de control de acceso, sistema de extinción de incendios, entre otros que protejan el lugar. El acceso estará restringido. El Proceso de Soporte tecnológico es el área encargada de la administración y de la seguridad de los equipos, conexiones y demás elementos del lugar.
- Los gabinetes de comunicaciones y cableado estructurado que se encuentra ubicados en las sedes de la Corporación deben estar resguardados bajo medidas de seguridad adecuadas para estos sitios. El acceso estará restringido.
- Los funcionarios, pasantes o personal de apoyo son responsables de hacer buen uso de las redes de datos y de los demás equipos de conectividad de la Entidad (Router, Switch, módems, entre otros) y de reportar cualquier anomalía al proceso de Soporte Tecnológico.
- Como requisito para interconectar la red de Corpoboyacá con las de terceros, los sistemas de comunicación de terceros deben cumplir con requisitos básicos de seguridad establecidos por Corpoboyacá.
- El proceso de Soporte Tecnológico es el área encargada de proveer y mantener las conexiones de las redes de datos de la entidad y de establecer nuevos mecanismos de conexión.
- Al momento de instalar o cambiar el cableado estructurado de la red interna de datos se debe tener en cuenta las consideraciones técnicas de las normas vigentes de cableado estructurado y del reglamento técnico de Instalaciones eléctricas RETIE

### **5.2.11 POLITICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**

**Propósito:** Establecer lineamientos para promover que la seguridad sea parte integral de los sistemas de información durante las fases de adquisición, desarrollo y mantenimiento de los sistemas de información.

#### **REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**

- En la adquisición de sistemas de información se debe contemplar las especificaciones de requisitos de seguridad de la información. Se deben contemplar las etapas que sean necesarias en la adquisición de sistemas de información como: Planificación, análisis, estudios de necesidades y funcionalidades, establecimiento de requisitos funcionales y no funcionales, adquisición del sistema, implementación, pruebas, despliegue del sistema en producción, soporte y mantenimiento del sistema. La Adquisición de sistemas de información deberá tener concepto técnico aprobatorio del proceso de Soporte Tecnológico.

- El desarrollo de sistemas debe ser llevado a cabo por un equipo de Gestión y desarrollo de proyectos de software y contemplar como mínimo las siguientes fases generales de desarrollo de sistemas: Especificación de requisitos funcionales y no funcionales (rendimiento, seguridad y disponibilidad), análisis del sistema, diseño, desarrollo, pruebas, documentación, instalación, despliegue en producción, soporte y mantenimiento. En todos los casos el desarrollo de sistemas de información, herramientas de apoyo o componentes deben tener concepto técnico aprobatorio del proceso de Soporte Tecnológico, a fin que sean integrados a la gestión de activos TIC.
- El soporte y mantenimiento de sistemas de información de la Corporación son necesarios para su normal funcionamiento, por lo tanto, el Proceso de Soporte Tecnológico será el área encargada de establecer o apoyar los criterios para el soporte y mantenimiento de los sistemas de información a cargo de los proveedores o terceros.
- Todos los Sistemas de Información debe incluir como mínimo las siguientes funcionalidades para la gestión y seguridad de usuarios: Acceso y Administración de usuarios, Rol de Usuario, Log o registro de Operaciones

## 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).
- **Activo crítico.** Instalaciones, sistemas y equipos que por cualquier motivo sino se encuentran disponibles o en funcionamiento, afectan el cumplimiento de los objetivos estratégicos de la entidad.
- **Causa** (contexto del riesgo): Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Ciberseguridad:** Es el proceso de proteger sistemas de información, redes de datos, programas de computador y otros activos de información de ataques digitales.
- **Cifrado.** Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

- **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.
- **Criptografía:** Se ocupa del estudio de los algoritmos, protocolos y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.
- **Datacenter.** Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.
- **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.
- **Directorio activo (Active Directory).** Es un sistema que proporciona servicios de directorio en la red LAN, siendo capaz de crear objetos como usuarios, grupos y equipos en la red, proporcionando credenciales para el inicio de sesión en los equipos que se conectan a una red y con la capacidad de administrar y aplicar políticas a todos los equipos que sean registrados y conectados a la red, de asignar recursos como carpetas o unidades compartidas de red, impresoras, equipos y pueden otorgar permisos sobre los objetos.
- **Dispositivos móviles.** Equipo celular (Smartphone), equipos portátiles, tablets, u otros dispositivos cuyo concepto principal sea la movilidad, el cual permite almacenamiento limitado, acceso a internet y capacidad de procesamiento.
- **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.
- **Funcionalidades básicas para la gestión y seguridad de usuarios:**
  - **Acceso y Administración de usuarios:** Establece la gestión de registro de usuarios y acceso mediante usuario y clave cifrada, parámetros sobre longitud mínima de las contraseñas, frecuencia de cambio, periodos de vigencia, activación e inactivación de usuarios, entre otras.
  - **Rol de Usuario:** Contar con roles predefinidos o un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. También deben permitir rol de usuario de Administración.
  - **Log o registro de Operaciones:** Hace referencia a las pistas o registros de los sucesos relativos a la operación dentro del sistema.

- **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.
- **Infraestructura crítica:** Es el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una nación. (Resolución CRC 2258 de 2009).
- **Impacto (contexto del riesgo):** 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.** Es una orientación de carácter general, corresponde a una disposición o directriz que debe ser implementada en las entidades del Estado.
- **Licencia Pública General de GNU:** La Licencia Pública General de GNU o más conocida por su nombre en inglés GNU General Public License (o simplemente sus siglas en inglés GNU GPL) es una licencia de derecho de autor ampliamente usada en el mundo del software libre y código abierto y garantiza a los usuarios finales (personas, organizaciones, compañías) la libertad de usar, estudiar, compartir (copiar) y modificar el software.
- **Medio removible:** Los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente. Los dispositivos móviles más comunes son: Memorias USB, Discos duros extraíbles, DVD y CD.
- **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.
- **Plan de contingencia:** Es una estrategia que se compone de una serie de procedimientos o pasos que facilitan una solución alternativa que permite restituir rápidamente el funcionamiento de los servicios críticos de la entidad ante la eventualidad falla o interrupción que lo afecte de forma parcial o total.
- **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.
- **Probabilidad:** Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año
  - **Recurso Informático:** Elementos informáticos (base de datos, servidores, computadores, aplicaciones informáticas, dispositivos y elementos de cómputo, redes de datos, servicios y sistemas de información y comunicaciones) que facilitan o proveen servicios informáticos.
  - **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
  - **Riesgo Inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
  - **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente
  - **Sistema de información.** Un sistema de información es un conjunto de componentes que interactúan entre sí con un fin común. En informática, los sistemas de información ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización.
  - **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.
  - **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 la gerencia de las organizaciones determinar con objetividad qué información requiere ser protegida, por qué debe ser protegida, de qué debe ser protegida y cómo 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.
  - **Correo no deseado o Spam** (correo basura, correo no deseado o correo no solicitado). Comunicaciones no solicitadas que se envían de forma masiva por Internet o mediante otros

sistemas de mensajería electrónica. Hacen referencia a los mensajes de correo electrónico no solicitados, no deseados o con remitente no conocido (o incluso correo anónimo o de falso remitente), habitualmente de tipo publicitario, generalmente son enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

- **Tecnologías de la Información:** Tecnologías de la información y las Comunicaciones - TIC, agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones, principalmente en la informática, internet y telecomunicaciones.
- **Tratamiento del riesgo.** Proceso de selección e implementación de medidas para modificar el riesgo.
- **TRD.** Constituyen un instrumento archivístico que permite la clasificación documental de la entidad, acorde a sus estructura orgánico – funcional, e indica los criterios de retención y disposición final de los documentos por cada una de las agrupaciones documentales, así como un instrumento de clasificación de los activos de información de la Entidad.
- **Cuadro de clasificación documental.** Instrumento que refleja la jerarquización dada a la documentación producida por la Corporación Autónoma Regional de Boyacá – Corpoboyacá, en el que se registran las secciones, series y Subseries documentales, con sus respectivos códigos.
- **Inventario documental.** Instrumentos de recuperación de información que describe las series, Subseries, asuntos del fondo documental de la Corporación Autónoma Regional de Boyacá.
- **VPN.** Red virtual privada por sus siglas en ingles Virtual Private Network
- **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. CAMBIOS EFECTUADOS

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
0	Establecimiento de política general y estructuración de políticas específicas de seguridad de la información.	09/02/2023