LISTA DE VERSIONES

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
0	09/Sep/2019	El Manual inicia en versión 0 debido al rediseño institucional adoptado a través de la ordenanza N° 049 de diciembre de 2018, al nuevo mapa de procesos según Decreto N° 475 del 23 de Julio de 2019 y al Instructivo de ELABORACIÓN Y ACTUALIZACIÓN DE DOCUMENTOS DEL SISTEMA DE GESTIÓN, el cual hace parte del subproceso Direccionamiento y mejoramiento de Métodos y Sistemas de Gestión.
1	19/Nov/2021	Se actualizan metas para la articulación con el nuevo programa de gobierno, se agrega normatividad de Teletrabajo, Trabajo en casa y estándar de continuidad de negocios. Se modifican políticas y directrices como: Protección del derecho de acceso a la información, Privacidad y confidencialidad de la información, Control de acceso a la información y a las aplicaciones, Seguridad en telecomunicaciones y servicios asociados, Seguridad de equipos de cómputo, Uso de correo electrónico y otros servicios, Gestión de incidentes, Continuidad del negocio, entre otras. Se agregan políticas de Seguridad de los recursos humanos, teletrabajo, trabajo en casa; adquisición, desarrollos y mantenimiento de sistemas; Gestión de activos de información.

CONTENIDO

1. OBJETIVOS

Definir políticas de seguridad de uso y administración de Tecnologías de Información y comunicación de la Gobernación de Boyacá, describiendo el manejo adecuado de las mismas, y estableciendo objetivos organizacionales para la protección de los activos de información, así como las responsabilidades y los derechos que deben conocer y cumplir los usuarios clientes internos y externos, custodios y administradores de la infraestructura tecnológica para lograr que los recursos tecnológicos de la entidad presten su servicio de manera accesible, confiable y oportuna.

La Gobernación de Boyacá, para el cumplimiento de su misión, visión, objetivo estratégico y apegada a sus valores corporativos, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

- Minimizar el riesgo en las funciones más importantes en la Entidad
- Cumplir con los principios de seguridad de la información
- Cumplir con los principios de la función administrativa
- Mantener la confianza de los ciudadanos, funcionarios y otras partes interesadas
- Apoyar la innovación tecnológica
- Implementar el Sistema de Gestión de Seguridad de la Información
- Proteger los activos tecnológicos
- 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 y clientes de la Gobernación de
- Boyacá
- Garantizar la continuidad del negocio frente a incidentes.

2. ALCANCE

Este documento hace parte integral de la política general de seguridad de la Información la cual se ha definido como la declaración general que representa la posición de la administración de la Gobernación de Boyacá con respecto a la protección de los activos de información (personal, la información, los procesos, las tecnologías de información incluido el hardware y el software), a la implementación del Sistema de Gestión de Seguridad de la Información y el apoyo, generación y publicación de sus políticas, procedimientos e instructivos. Esto ayuda a propender para que la información de la entidad se provea con requerimientos de confidencialidad, integridad y disponibilidad.

La seguridad de la información es un esfuerzo de equipo. Se requiere la participación y apoyo de todos los miembros de la organización que trabajan con sistemas de información o utilizan la Infraestructura Tecnológica de la Gobernación de Boyacá, es decir, que las políticas definidas en el presente documento aplican a todos los funcionarios públicos, contratistas, proveedores y demás usuarios internos y externos de las tecnologías de Información de la entidad.

Esta política se aplica a toda la infraestructura tecnológica (tal como hardware, software y redes de datos) y a todos los activos de información operados por los funcionarios y otros usuarios de la Gobernación de Boyacá que hacen uso de esta infraestructura. Se incluyen también aquellos equipos de cómputo personales que no son propiedad de la entidad pero que están al servicio de la misma y afectan la red de datos interna.

Se quiere también con esta política dar cumplimiento a los lineamientos nacionales de la Política de Gobierno Digital para la implementación del Modelo de Seguridad de la Información y establecer directrices de continuidad y recuperación de los servicios TI en caso de desastres.

Todos los usuarios cuentan con un documento que incluye los requisitos de la política de seguridad de la información y otra documentación relacionada. Quienes deliberadamente o por negligencia infrinjan las políticas de seguridad de la información estarán sujetos a acciones de seguimiento y disciplinarias según sea el caso.

Este documento es la base para la generación de un plan de seguridad de la información que permita establecer procedimientos y operaciones para la aplicación de cada una de las políticas de seguridad que se definen aquí.

3. DEFINICIONES

Acceso lógico controlado: Un sistema informático debe ser utilizado solamente por aquellas personas autorizadas, debe procurar detectar y excluir las no autorizadas. El acceso lógico por lo tanto es controlado generalmente insistiendo en un procedimiento de la autentificación para establecer con un cierto grado de confianza la identidad del usuario, concediendo privilegios autorizados a esa identidad.
Ataque cibernético: intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo con el objetivo de causar daño a un sistema, robar información del mismo o utilizar sus recursos de forma no autorizada.
Autenticación de usuario: (en inglés **Login** – Logearse) Es el proceso de verificar la identidad digital de un usuario a través de una petición para conectarse o de un remitente cuando hace una petición de comunicación controlándose el acceso hacia algún recurso. El usuario o remitente siendo autenticado puede ser una persona que usa un computador, un computador por sí mismo o un programa del computador. Una contraseña o clave (en inglés password) es una forma de autenticación que utiliza información secreta.
Brecha de seguridad: deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en si misma, sea o no protegida por reserva legal.
Certificado Digital: un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.
Cifrar: También denominado encriptar, quiere decir transformar un mensaje o un archivo en un documento no legible, y el proceso contrario se llama descifrar. Los sistemas de ciframiento se llaman `sistemas criptográficos". Es un mecanismo de control para proteger los datos que se almacenan o distribuyen como mensajes o archivos.
Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Debe entonces entenderse el “dato personal” como una información relacionada con una persona natural (persona individualmente considerada).
Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio ya su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Documento de archivo: Es el registro de información producida o recibida por una entidad pública o privada en razón de sus actividades o funciones.
Identificación de usuario: Para que los usuarios puedan obtener seguridad, acceso a un sistema informático, administración de recursos, etc., dichos usuarios deberán identificarse a través de una cuenta de usuario autorizada; normalmente la identificación de un usuario es definida por un Administrador del Sistema.
Incidente: Evento que pone en riesgo la seguridad o disponibilidad de un sistema de cómputo.
Información: Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.
Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.
Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley 1712 de 2014.
Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014.
Intrusión: Es una secuencia de acciones realizadas por un adversario malicioso que resulta en una ocurrencia de amenazas de seguridad hacia un equipo de cómputo o una red de cómputo. Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.
ISO/IEC 27000: Es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.
No repudio: este mecanismo genera registros especiales con alcances de "prueba judicial" acerca de que el contenido del mensaje de datos es la manifestación de la voluntad del firmante y que se atiene a las consecuencias de su decisión.
Piratería: Se refiere a la reproducción y copia ilegal de obras literarias, musicales, audiovisuales y de software, sin permiso del titular de los derechos de autor o autorización legal. Abarca tanto la copia como la venta, distribución, almacenamiento, transporte, y en general la comercialización del producto ilegal.
Política: son instrucciones que indican la intención de la alta gerencia respecto a la operación de la organización.
Preservación a largo plazo: Conjunto de acciones y estándares aplicados a los documentos durante su gestión para garantizar su preservación en el tiempo, independientemente de su medio y forma de registro o almacenamiento.
Propiedad intelectual: Disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humanos, dignos de reconocimiento jurídico, la cual comprende: el derecho de autor y los derechos conexos; la propiedad industrial (que comprende la protección de los signos distintivos, las nuevas creaciones, los circuitos integrados, los secretos industriales); y las nuevas variedades vegetales.
Publicar o divulgar: Significa poner a disposición en una forma de acceso general a los miembros del público e incluye la impresión, emisión y las formas electrónicas de difusión.
Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.
Red de telecomunicaciones: Conjunto de elementos que permite la transmisión de señales entre dos o más puntos, fijos o móviles, terrestres o espaciales, a través de la cual se prestan servicios de telecomunicaciones.
Usuario final: Persona o personas que operan de manera directa una aplicación informática, producto de software o un servicio de TI.

RPO: Objetivo de Punto de Recuperación (Recovery Point Objetive) se determina en base a la pérdida aceptable de los datos en el caso de una interrupción de las operaciones. Ello indica el punto más anticipado en el tiempo al cual es aceptable recuperar los datos.
RTO: Objetivo de Tiempo de Recuperación (Recovery Time Objetive) se determina en base al tiempo improductivo aceptable en el caso de una interrupción de las operaciones. Ello indica el punto más anticipado en el tiempo en que las operaciones de la Entidad deben retomarse después del desastre.
Tratamiento de datos personales: Se refiere a la utilización, recolección, almacenamiento, uso, circulación y supresión de los datos personales que se encuentran registrados en cualquier base de datos o archivos por parte de entidades públicas o privadas y cuyo procesamiento sea utilizando medios tecnológicos o manuales.
Tratamiento de datos personales: Se refiere a la utilización, recolección, almacenamiento, uso, circulación y supresión de los datos personales que se encuentran registrados en cualquier base de datos o archivos por parte de entidades públicas o privadas y cuyo procesamiento sea utilizando medios tecnológicos o manuales
Usuario final: Persona o personas que operan de manera directa una aplicación informática, producto de software o un servicio de TI.
Usuario administrador de sistemas: Es un profesional universitario o especializado que se ha formado y entrenado en áreas del conocimiento: ingeniería del software, gestión administrativa empresarial, gestión de bases de datos, gestión de redes de datos y telecomunicaciones.
Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios de la GOBERNACIÓN DE BOYACÁ, pero que por las actividades que realizan en la Entidad, deben tener acceso a Recursos Informáticos.

Definiciones tomadas del estándar ISO/IEC 27000, ley 1581 de 2012, decreto 1377 de 2013, ley 1712 de 2014, artículo superintendencia de industria y comercio (SIC).

4. DOCUMENTOS RELACIONADOS

- Modelo de seguridad de la información para la Política de Gobierno Digital
- Manual de Gobierno Digital - Implementación de la Política de Gobierno Digital
- Política general de Seguridad y privacidad de la información
- Política de gestión de riesgos de seguridad digital
- Procedimiento de seguridad y privacidad de la información
- Procedimiento de continuidad de servicios (del negocio) y recuperación de desastres
- Programa de gobierno Boyacá tierra que sigue avanzando 2020 – 2023

5. CONDICIONES GENERALES

Normatividad:

- Ley 527 de 1999 Ley de comercio electrónico
- Ley 734 de 2002 Código disciplinario único
- Ley 1221 de 2008 Regulación del teletrabajo
- Ley 1266 de 2008 Habeas Data
- Ley 1273 de 2009 Código penal en lo referente a la protección de la información y de los datos
- Ley 1581 de 2012 Ley de protección de datos personales
- Ley 1474 de 2011 Estatuto anticorrupción - riesgo de corrupción sobre sistemas de información

- Ley 1437 de 2011 Código de procedimiento administrativo y de lo contencioso administrativo y reformas
- Ley 1712 de 2014 Ley de transparencia y del derecho de acceso a la información
- Ley 2088 de 2021 Regulación del trabajo en casa
- Decreto 103 de 2015 Reglamenta parcialmente la Ley de transparencia
- Decreto 2609 de 2012 Preservación de documentos en ambientes electrónicos
- Decreto 1377 de 2013 Protección de datos sensibles y debido tratamiento
- Decreto 415 de 2016 Lineamientos para el fortalecimiento institucional en materia de TIC
- Decreto 1008 de 2018 Lineamientos generales de la política de gobierno digital
- Resolución 1519 de 2020 Estándares y directrices para publicar información
- ISO/IEC 27001: 2013 Estándar internacional para sistemas de gestión de seguridad de la información
- ISO 22301:2019 Estándar internacional para seguridad y resiliencia en la continuidad del negocio
- CONPES 3701 de 2011 Lineamientos de la política para ciberseguridad y ciberdefensa
- CONPES 3854 de 2016 Política nacional de seguridad digital
- CONPES 3995 de 2020 Política nacional de confianza y seguridad digital

Metas de la Política de Seguridad

En el Programa de Gobierno Boyacá tierra que sigue avanzando 2020 – 2023 se estableció el subprograma "Gobierno Digital avanza con seguridad digital" que tiene por objetivo Desarrollar un gobierno digital con estrategia de TI articulada a los subprocesos de negocio a través de planes para aseguramiento de los activos de información de la entidad. Para ello se establecieron las Metas:

- El 90% del Aseguramiento de los activos de información de la entidad diagnosticado
- El 75% del Plan de control operacional del Sistema de Gestión de seguridad de la información (SGSI) implementado
- Una solución tecnológica como iniciativa que apoya el Teletrabajo en el marco d un Sistema de Gestión de la continuidad del negocio (SGSI) implementada
- EL 55% del plan de tratamiento de riesgos de seguridad digital implementado

Adicionalmente se tiene como meta desarrollar cada año el Programa de sensibilización y formación en seguridad de la información para que los usuarios apropien el buen uso de la las Tecnologías de la Información y Comunicación de la Gobernación de Boyacá, y conozcan las responsabilidades y las medidas que se deben adoptar para proteger los activos de TI y evitar pérdidas y/o divulgación no autorizada.

De otro lado, se cuenta con metas en aspectos de seguridad y privacidad de la información que la Entidad territorial debe cumplir por normatividad nacional a través de la Política de Gobierno Digital.

La gestión de Tecnología de Información y Comunicación de la Gobernación de Boyacá propone esfuerzos de seguridad digital a través de la Dirección de Sistemas de Información con el proceso de Gestión de las tecnologías de la información dentro del Modelo Integrado de Planeación y Gestión MIPG, para la implementación de la política de seguridad y privacidad de la información.

Marco de gestión de la seguridad y gestión de recursos de TI

De acuerdo a la normativa que plantea el Gobierno nacional bajo el Decreto 1008 de 2018 se establece un marco para la Gestión de Tecnologías de Información y tareas de institucionalidad de TI para que las Entidades del Estado permitan el mejoramiento de la planificación, organización, coordinación, gestión y control de la estrategia de uso y apropiación de TI.

El **GCIO (Government Chief Information Officer)** Es el encargado de la Gestión estratégica de TI quien lidera estrategias de gestión de información para garantizar la pertinencia, calidad, oportunidad, **seguridad** e intercambio con el fin de lograr un flujo eficiente de información disponible para el uso en la gestión y la toma de decisiones en la entidad, art. 2.2.35.3 inciso 11 Decreto 415 de 2016. El GCIO en la Gobernación de Boyacá es el Director de Sistemas de Información que junto con el Secretario de TIC y Gobierno abierto son responsables de formular las políticas de seguridad de la Información propuestas ante la Mesa técnica de Gobierno y Seguridad Digital para su aprobación.

La Mesa técnica de Gobierno y Seguridad Digital es responsable de establecer y mantener las políticas de seguridad de la información, identificando estándares, normas, directivas en la materia y documentar su aplicabilidad para los procesos de la Gobernación.

La Dirección de Sistemas de Información es la encargada de recordar regularmente a los empleados, contratistas y demás usuarios acerca de sus obligaciones con respecto a la seguridad de los activos de información para fortalecer el buen uso y apropiación.

La Dirección de Sistemas de Información a través de un plan de seguridad de la información diseña y ejecuta la forma de aplicar cada una de las políticas de seguridad. Las responsabilidades del personal y de los dueños de proceso se definen en dicho plan y también en la Política general de seguridad y privacidad de la información.

La Oficina Asesora de Control Interno de Gestión se encarga de velar por el cumplimiento de las políticas, procedimientos y la legislación aplicable a tecnologías de la información y seguridad de la información.

La investigación de incidentes de seguridad de información está a cargo tanto de la Dirección de Sistemas de Información, como de los entes externos que tengan orden judicial para hacerlo.

La acción disciplinaria en respuesta a las violaciones de las normas de seguridad de información es responsabilidad de la Oficina Asesora de Control Interno Disciplinario, actuando conjuntamente con la Dirección General de Talento Humano.

Las políticas que figuran en este documento forman parte integral de La política general de seguridad y privacidad de la información. Esta ha sido aprobada, apoyada y defendida por la alta dirección de la Gobernación de Boyacá, aportando al cumplimiento de las metas de la Gobernación. El interés en su aplicación está en brindar un servicio de calidad, y fortalecer el modelo fundamentado en la gestión de conocimiento, dando un valor crítico y naturaleza sensible a la información.

Gestión de actualizaciones de las políticas de seguridad

De requerirse alguna actualización o cambio en el manual de políticas de seguridad de la información, deberá ser solicitado a la Mesa técnica de Gobierno y Seguridad Digital por medio de los canales electrónicos dispuestos para este propósito: correo electrónico despacho.tic@boyaca.gov.co, seguridad.digital@boyaca.gov.co, o a través de oficio remisorio mediante el Sistema de Gestión Documental, que se encargará de la revisión, investigación y aprobación de actualizaciones. En la solicitud se deberá detallar la política de la cual se solicita actualización y referenciar un documento que soporte o justifique la solicitud. Para el caso de sugerencias o resolución de dudas, también se pueden utilizar los canales electrónicos señalados.

Gestión de excepciones de las políticas de seguridad

En caso que existan situaciones potenciales que impidan el cumplimiento de las políticas de seguridad de la información, los Secretarios o Directores de la Gobernación de Boyacá podrán enviar la solicitud de la excepción por medio de los canales electrónicos dispuestos para este propósito: correo electrónico despacho.tic@boyaca.gov.co,

seguridad.digital@boyaca.gov.co, o a través de oficio remisorio mediante el Sistema de Gestión Documental, y esta será revisada por la Mesa técnica de Gobierno y Seguridad Digital que se encargará de la investigación y aprobación de excepciones.

6. POLÍTICAS DE OPERACIÓN

POLÍTICA 1: CLASIFICACIÓN, ORDENACIÓN DE LA INFORMACIÓN Y DERECHO DE ACCESO

Directriz de clasificación de la información

La clasificación de la información constituye un elemento importante de la gestión de riesgos, ya que determina las necesidades, la prioridad y el grado de protección necesario para cada tipo de información. La Gobernación de Boyacá ha adoptado una estructura de información donde considera la información calificada conforme a la ley de transparencia. Esta estructura define el nivel adecuado de protección e informa a los responsables de cualquier medida especial o tratamiento requerido.

Para establecer los tipos de información se tendrá en cuenta el Decreto 2609 de 2012 que en materia de gestión documental hace referencia a la información producida y/o recibida por las entidades públicas, sus dependencias y servidores públicos, y en general por cualquier persona que desarrolle actividades inherentes a la función de dicha entidad o que hayan sido delegados por ésta, independientemente del soporte y medio de registro (análogo o digital) en que se produzcan y que se conservan en : a. Documentos de Archivo (físicos y electrónicos). b. Archivos institucionales (físicos y electrónicos). c. Sistemas de Información Corporativos. d. Sistemas de Trabajo Colaborativo. e. Sistemas de Administración de Documentos. f. Sistemas de Mensajería Electrónica. g. Portales, Intranet y Extranet. h. Sistemas de Bases de Datos. i. Disco duros, servidores, discos o medios portables, cintas o medios de video y audio (análogo o digital), etc. j. Cintas y medios de soporte (back up o contingencia). k. Uso de tecnologías en la nube.

Según el tipo de información que los usuarios y custodios manejen, toda la información debe integrarse en una de las siguientes clasificaciones establecidas por la Ley 1712 de 2014:

- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal, art 6. Ley 1712 de 2014. **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio ya su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva, señalados en el art.3 del Decreto 1377 de 2013.

- **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el art.18 de la ley 1712 de 2014; es decir, se exceptúa acceso en caso de daño a los siguientes derechos: intimidad, la vida, la salud o la seguridad, los secretos comerciales, industriales y profesionales. **Datos sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos, señalados en el art.3 del Decreto 1377 de 2013.

- **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la

totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014; es decir, se exceptúa acceso en caso de las siguientes circunstancias: a) La defensa y seguridad nacional. b) La seguridad pública. c) Las relaciones internacionales. d) La prevención, investigación y persecución de los delitos y las faltas disciplinarias. e) El debido proceso y la igualdad de las partes en los procesos judiciales. f) La administración efectiva de la justicia. g) Los derechos de la infancia y la adolescencia. h) La estabilidad macroeconómica y financiera del país. i) La salud pública.

Directriz de clasificación y ordenación de archivos electrónicos

Los usuarios deben propender mantener una ordenación de archivos electrónicos según se indique en la Tabla de Retención Documental (TRD) definida y aprobada por la Gobernación de Boyacá, los administradores de los activos de información deberán utilizar un almacenamiento estructurado y racional de carpetas, subcarpetas y archivos electrónicos, que tengan nombres cortos y no estén ubicados en más de un cuarto subnivel de almacenamiento (subcarpetas). El nombre de un archivo, incluida la ruta desde el directorio raíz, la carpeta y las subcarpetas NO deberá superar los 255 caracteres; si esta longitud es muy extensa, puede afectar procesos de backup, copia, migración, restauración, transferencia o compatibilidad entre sistemas de archivos.

Así que, se tendrán en cuenta los criterios de clasificación, ordenación y descripción de los archivos conforme al Acuerdo 005 de 2013 del AGN (Archivo General de la Nación), y la estructura semántica para nombrar los documentos electrónicos de archivo de la Guía para la gestión de documentos y expedientes electrónicos del MinTIC.

Los documentos electrónicos y la información en ellos contenida, deberá estar disponible en cualquier momento, mientras la entidad está obligada a conservarla, de acuerdo con lo establecido en las Tablas de Retención Documental (TRD), y conforme se establece en el Decreto 2609 de 2012.

Directriz de protección del derecho de acceso a la información

La información a ser publicada y divulgada en el marco de una transparencia activa, deberá seguir las directrices generales para la publicación que establece el Decreto reglamentario 103 de 2015:

La información mínima obligatoria se deberá publicar en sitio web oficial en una sección identificada con el nombre "Transparencia y acceso a información pública" conforme lo establece el art. 4 del decreto, relacionada con aspectos organizativos, presupuestales, normatividad aplicable, esquemas de publicación de información, registro de activos de información, programa de gestión documental, tablas de retención documental, informe de solicitudes de acceso a la información; así mismo, se deberá publicar el directorio de información de servidores públicos, empleados y contratistas (art. 5), los trámites y servicios que se adelantan (art 6), la información de gestión contractual (art. 7), documentos o informes que prueben la ejecución de contratos (art 8), procedimientos, lineamientos y políticas en materia de adquisición y compras (art 9), plan anual de adquisiciones (art.10), datos abiertos (art 11).

También, se deberá dar cumplimiento a las directrices y lineamientos de la Resolución 1519 de 2020 que define estándares de publicación y divulgación de información, directrices de accesibilidad de contenidos web, condiciones técnicas y de seguridad digital, y condiciones de publicación de datos abiertos.

En cuanto a solicitudes de información pública en el marco de una transparencia pasiva, se deberá seguir las directrices que también establece el Decreto reglamentario 103 de 2015:

Se deberán considerar y divulgar los medios idóneos para recibir solicitudes de información pública (art. 16), permitir hacer seguimiento a las solicitudes de información pública (art.17), permitir solicitudes de acceso a información con identificación reservada (art. 18), hacer gestión y dar respuesta a las solicitudes de acceso (art. 19 y 20). Se deberá hacer seguimiento a la gestión de la información pública (art. 51, 52).

POLÍTICA 2: CONTROL DE ACCESO A LA INFORMACIÓN Y A LAS APLICACIONES

Todos los funcionarios públicos, contratistas, proveedores y demás usuarios de la Infraestructura de Tecnología de Información y Comunicación de la Gobernación de Boyacá pueden tener acceso sólo a la información necesaria y suficiente para el desarrollo de sus actividades. El otorgamiento de acceso a la información está regulado por niveles o perfiles de acceso que define el dueño del proceso o subproceso.

Tanto los usuarios externos como internos de la Gobernación de Boyacá, que requieran ingresar a los sistemas de información de la entidad, deberán estar autorizados por el Director del área o dueño del proceso o subproceso, quien realizará la solicitud a través de los canales dispuestos para tal fin, los detalles se establecerán en el instructivo definido para la administración de cuentas de usuario y perfiles de acceso a los sistemas.

Todas las Tecnologías de Información y Comunicación (equipos de cómputo, software del sistema, software de aplicaciones, bases de datos, etc.) deben contar con mecanismos de identificación, autenticación y roles de privilegios de usuario apropiados según la clase de información y el tratamiento que se autorice a la misma. No se podrá eliminar cuentas de usuarios de ningún sistema, solamente se desactivará el acceso cuando se requiera.

Las identificaciones de usuario deben individualizar a usuarios específicos y ser utilizada con el fin de permitir el acceso a los sistemas de acuerdo a las funciones, responsabilidades y actividades de dichos usuarios. Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y claves personales.

Toda vez que algún trabajador deje de prestar sus servicios a la Entidad, debe asegurar la entrega total de la información que gestionó durante el ejercicio de sus funciones. Una vez retirados se obligan a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la Entidad, por el tiempo de clasificación o reserva establecido en el catálogo de activos de información del proceso o subproceso.

Todas las prerrogativas para el uso de los sistemas de información de la Gobernación de Boyacá terminan inmediatamente después de que el trabajador cesa de prestar sus servicios a la Entidad. Para el cumplimiento de esta directriz, cada uno de los Directores de las Secretarías o Dependencias está obligado a solicitar a la Dirección de Sistemas de Información, o a la Sectorial que administre ciertos sistemas, la desactivación de cuentas de acceso (especificando los sistemas en los que se tenía uso) a través de los canales dispuestos para tal fin. El director que no cumpla esta política se responsabiliza de las acciones que se generen por la omisión.

Mediante el monitoreo de registros automáticos de eventos en las diversas plataformas tecnológicas y sistemas se efectuará seguimiento a los accesos realizados por los usuarios a la información y recursos de TI de la Entidad, con el objeto de minimizar riesgos tecnológicos de la información. Cuando se presenten eventos que pongan en riesgo la integridad, disponibilidad, confiabilidad, confidencialidad, eficiencia y/o efectividad de la información, se deberán documentar y realizar las acciones tendientes a su solución.

El nivel de Superusuario de cada uno de los sistemas críticos deberá tener un control dual, de tal forma que exista una conciliación de las actividades realizadas en el sistema por otro administrador. No se debe crear o disponer de cuentas de Superusuario por más de dos Administradores para cada Sistema de Información, debido a que el control se perdería.

Todos los equipos servidores deberán tener controles de acceso para garantizar la integridad y disponibilidad de la información, archivos electrónicos, bases de datos, y aplicativos de Sistemas de información almacenados y configurados en dichos equipos.

Directriz de contraseñas para acceso a la información y a las aplicaciones

La autenticación (clave o contraseña), para el acceso a un sistema o recurso informático, debe ser definida por el usuario de las Tecnologías de Información de la Gobernación de Boyacá, y es considerada como un dato sensible; es el usuario quien tiene la responsabilidad exclusiva de manejarla, no divulgarla, ni compartida.

Al establecer la contraseña para acceso a un sistema, ésta debe ser fácil de recordar para el usuario, pero difícil de adivinar por un extraño; no utilizar palabras únicas que se encuentren en un diccionario o que se refieran a datos personales o familiares; no utilizar solo números; se deben combinar caracteres alfanuméricos; tener al menos una mayúscula y una minúscula; y como mínimo debe tener una longitud de ocho (8) caracteres.

Las contraseñas deben modificarse a intervalos regulares, preferiblemente cada 180 días o menos para el caso de aquellos sistemas que no exijan un cambio periódico obligado.

Las contraseñas no deberán ser almacenadas en ningún formato legible en archivos desprotegidos, almacenados en lugares o carpetas donde las personas no autorizadas puedan encontrarlas. Las contraseñas en ningún momento deberán estar escritas y a la vista, como en monitores de computadoras y escritorios.

Si un usuario tiene acceso a varios sistemas de información, estará obligado a definir una contraseña diferente para cada uno, a menos que se tenga establecido y configurado el Directorio activo en la Entidad y articulado con cada sistema.

Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas temporales suministradas de acceso a la red, sistemas de información, plataformas, aplicaciones, entre otros.

POLÍTICA 3: PRIVACIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

Directriz de privacidad de la información y tratamiento de los datos personales

En el catálogo de activos de información definido por cada proceso y subproceso de la Entidad se deberá declarar aquellos activos que contienen datos personales en general, datos personales de niños, niñas y adolescentes; la finalidad de la recolección de estos datos y si existe autorización para el tratamiento de estos datos, según aplique.

Los usuarios de bases de datos, archivos o sistemas de la entidad que realicen tratamiento de datos personales del ciudadano están obligados a cumplir las leyes 1266 de 2008, 1581 de 2012 y sus reformas, por las cuales se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial y de servicios, entre otras disposiciones.

El personal que tenga acceso a información sensible, a información de uso interno y a información de carácter personal del ciudadano deberá atender las implicaciones de la ley 1273 de 2009 y sus reformas, por medio de la cual se crea un nuevo bien jurídico tutelado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Se exige que todo tratamiento de datos de carácter personal del ciudadano, realizado por el usuario o responsable, cumpla pautas éticas y legales. Para ser lícito el tratamiento de datos personales deberá basarse en el consentimiento informado del interesado, según aplique. Los principios y las normas sobre protección de datos de carácter personal del ciudadano no buscan impedir el uso de los mismos sino garantizar que su uso evite conductas indebidas que se traducen en amenazas o vulnerabilidades de los derechos fundamentales de la persona.

Toda la información que sea sensible, crítica o valiosa con datos personales almacenada en un equipo servidor o en un equipo cliente deberá estar sometida a mecanismos de protección para garantizar que no sea inapropiadamente descubierta, modificada, borrada y que pueda ser recuperable.

Si una Entidad, empresa o personal externo requiere acceso a información sensible o crítica con datos personales, se deben suscribir acuerdos de confidencialidad y de no divulgación para la salvaguarda de la información, así como cláusulas de cumplimiento de la normatividad vigente para la Entidad y obtener la autorización de los titulares de los datos, según sea el caso.

Cada sectorial de la Entidad deberá hacer registro de la caracterización de las bases de datos que contengan datos personales, de conformidad al art. 25 de la ley 1581, haciendo uso de la plataforma del Registro nacional de bases de datos dispuesta por la Superintendencia de Industria y Comercio (SIC), y registrar periódicamente las respectivas actualizaciones a que haya lugar por cambios que surjan en estas bases de datos. Las peticiones de protección de derecho Habeas Data deberán ser respondidas por cada sectorial o dueño de proceso quien es responsable de custodiar la información.

La Secretaría general en cabeza de la Subdirección de atención al ciudadano debe establecer la Política de tratamiento de datos personales de la Gobernación de Boyacá con el propósito de entregar la información necesaria y suficiente a los diferentes grupos de interés y ciudadanía en general sobre lineamientos que garanticen la protección de los datos personales que son objeto de tratamiento a través de los procesos, subprocesos, trámites y servicios de información de la Entidad, donde se dé cumplimiento a la normatividad de atención del derecho de Habeas Data de los titulares bajo criterios de recolección, almacenamiento, uso, circulación y supresión que se dará a los datos personales. Se deberá dejar a disposición la información necesaria y suficiente sobre los diferentes tratamientos y finalidades a los que serán objeto estos datos como entidad responsable del tratamiento de los mismos, y el procedimiento para atender los derechos de los titulares.

Directriz de confidencialidad de la información

Se debe dar cumplimiento a las directrices de confidencialidad de acuerdo al Artículo 34 de la Ley 734 de 2002 o Código disciplinario único, donde se establece que son deberes de todo servidor público:

- Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función en forma exclusiva para los fines a que están afectos.
- Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.

En virtud del Código disciplinario único, que regula los deberes de todo servidor público, y del código de procedimiento administrativo y de lo contencioso administrativo, que regula lo relacionado con la información reservada a que tenga acceso por razones de su función, se deberá garantizar la protección de la información por cuanto dicho aspecto está expresamente regulado en la ley y es de obligatorio cumplimiento por parte de todo servidor público.

Para el caso de contratistas, estos deberán aceptar y firmar el acuerdo de confidencialidad establecido para la protección de la información y los datos personales, así como el compromiso del cumplimiento de las políticas de seguridad y privacidad de la información de la Gobernación de Boyacá, ya sea en un documento anexo al contrato o dentro de las cláusulas del mismo.

El contratista debe guardar y mantener reserva de toda la información que sea de propiedad del Departamento de Boyacá o conozca en desarrollo del contrato, en especial cuando se trate de información sujeta a reserva legal o que sea clasificada (privada, semiprivada). Igualmente, una vez terminado un contrato el contratista está obligado a entregar los documentos, correspondencia y publicaciones que haya producido en el marco del mismo, y demás activos de información de propiedad del Departamento de Boyacá relacionados con el objeto del contrato; no debe quedarse con copia de aquellos que contengan información confidencial.

En consecuencia, tanto el funcionario público como el contratista o tercero contratado se obliga a:

- Proteger la información confidencial que el Departamento de Boyacá le comparta o suministre.
- Seguir las directrices establecidas en el manual de políticas de seguridad de la información y cumplir los procedimientos definidos en el plan de seguridad y privacidad de la información.
- No dar a conocer a terceros la información confidencial, sensible, critica, reservada o clasificada, que pueda perjudicar al Departamento de Boyacá.
- No dar a la información confidencial un uso distinto para el cual fue compartida o suministrada, salvo previa autorización por escrito del Departamento de Boyacá.
- Organizar y entregar toda la información archivada (física o digitalmente), utilizando la nemotecnia de las tablas de retención documental.
- No podrá realizar atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos en concordancia con la ley 1273 de 2009.
- Resarcir los perjuicios, por daño emergente y lucro cesante que llegare ocasionar la revelación, divulgación o utilización de la información de manera distinta en razón de su función o al objeto del contrato ya se por mera negligencia o de forma dolosa.

POLÍTICA 4: GESTION DE ACTIVOS DE INFORMACIÓN

La Entidad establece los métodos de identificación, clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades, manteniendo mecanismos acordes para el control de riesgos de la información.

Cada activo de información debe contar con un responsable, que asegure la protección de la información y los datos que son almacenados. Los custodios de la información deben garantizar que todos los activos de información reciban un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados. La política de propiedad intelectual de este documento establece los lineamientos referentes a la propiedad de los activos de información.

Se deberá definir un procedimiento que señale responsabilidades y tareas relacionadas con la Gestión de activos de tecnologías de la Información que contenga las pautas para efectuar el inventario o catálogo de activos de información, su

valoración y la gestión de riesgos de seguridad digital, el cual deberá ser aplicado por cada uno de los procesos y subprocesos de la entidad.

Cada proceso y subproceso deberá dar cumplimiento a los requerimientos legales de clasificación de activos de información, de recolección de datos personales; de igual forma, hacer la justificación con fundamentos jurídicos y constitucionales para información clasificada o reservada y la descripción de la finalidad para datos personales.

Con el fin de garantizar un apropiado nivel de protección de los activos de información, la Gobernación de Boyacá deberá establecer y dar cumplimiento a la Política de gestión de riesgos de seguridad digital y al Plan de tratamiento de riesgos de seguridad y privacidad de la información.

POLÍTICA 5: COPIAS DE SEGURIDAD DE ARCHIVO ELECTRÓNICO Y RETENCIÓN

En los sistemas de archivo electrónico implementados, se debe garantizar la autenticidad, integridad, confidencialidad y la conservación a largo plazo de los documentos electrónicos de archivo que de acuerdo con las Tablas de Retención Documental o las Tablas de Valoración Documental lo ameriten, así como su disponibilidad, legibilidad (visualización) e interpretación, independientemente de las tecnologías utilizadas en la creación y almacenamiento de los documentos (Art. 18 Decreto 2609 de 2012).

Las copias de seguridad (Backup) de la información y documentos en ambientes electrónicos generadas en la Gobernación de Boyacá tienen el propósito de preservar y retener datos por un periodo de tiempo determinado para precisamente garantizar la autenticidad, integridad, confidencialidad y conservación.

Se debe realizar copias de seguridad de los documentos de archivo, bases de datos y de la información más relevante de acuerdo a los tipos de información producida señalados en el Decreto 2609 de 2012, la clasificación y valoración de la información identificada en instrumentos de recolección de información señalados en la ley 1712 de 2014.

Según la clasificación de la información definida por los procesos y subprocesos de la Entidad, se deberán establecer las medidas de respaldo de la información a través de mecanismos como discos de almacenamiento, nube privada o medios de propiedad de la Entidad. Cada sectorial o área administradora de la información es responsable de definir e informar a la Dirección de Sistemas de Información cuál es la información que se encuentra y se protege en computadores de escritorio o en portátiles, a la cual se realiza copias de seguridad periódicas atendiendo a lo establecido en la Planeación de Continuidad del negocio de la Gobernación de Boyacá.

Los funcionarios públicos y contratistas son los encargados de los respaldos de la información que generan en los equipos que tengan asignados; deberán velar por la integridad y disponibilidad de la información que manejen, especialmente si dicha información está protegida por reserva legal o ha sido definida como clasificada o reservada.

En el Centro de Procesamiento de Datos (CPD) donde permanecen los Servidores de la Gobernación de Boyacá se deberán generar copias de seguridad (backups) periódicas de la información que ha sido almacenada a través de las aplicaciones que procesan información en las bases de datos y bodegas de datos, o a través de clientes que tienen allí carpetas de usuario remoto.

Las copias de seguridad deberán tener un nivel adecuado de protección tanto físico como ambiental y los medios o soportes deberán verificarse periódicamente para asegurar que pueden responder efectivamente en caso de ser requerida la recuperación de la información.

Se establecerá el periodo de retención de la información almacenada en medios o soportes de almacenamiento magnético, óptico o unidades de estado sólido, y su disposición final según las Tablas de Retención documental (TRD) de la Entidad y otros lineamientos en la materia definidos por el Archivo General de la Nación.

Se deberá definir procedimientos y/o instructivos que señalen responsabilidades y tareas relacionadas con la Administración de recursos de almacenamiento de información y la Gestión de continuidad de servicios para la operación del negocio en caso de situaciones de emergencia que requieran hacer uso de los backups.

POLÍTICA 6: CONTROL DE ACCESO FÍSICO

Directriz de seguridad de las instalaciones y ambientes de trabajo

Las oficinas administrativas, áreas de procesamiento de información, equipos tecnológicos y de soporte, información de medios físicos entre otros, son base para el cumplimiento de los objetivos de la Entidad, por tanto, se deben establecer y mantener controles para resguardar la seguridad de las instalaciones y ambientes de trabajo.

Las áreas de archivos centralizados, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información, conforme a la normatividad el AGN (Archivo General de la Nación).

Los Centros de Procesamiento de Datos (salas de servidores), los centros de cableado y demás áreas que la Dirección de Sistemas de Información considere críticas son lugares de acceso restringido y cualquier persona que ingrese a ellos deberá estar debidamente autorizada por el Dirección de Sistemas de Información y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares.

En los Centros de Procesamiento de Datos (salas de servidores), los centros de cableado y demás áreas que la Dirección de Sistemas de Información considere críticas para la administración de las Tecnologías de Información y Comunicación, deberán existir elementos de control de incendio, inundación y alarmas.

Los particulares, tales como familiares, conocidos de los funcionarios y externos sin relación contractual no están autorizados a acceder a los recursos informáticos instalados por la Entidad.

Directriz de seguridad de equipos de cómputo

Cuando se realicen procesos precontractuales y contractuales de suministro de equipos de cómputo para la Gobernación de Boyacá, teniendo en cuenta los riesgos tanto para seguridad física como para seguridad de salud en el trabajo que conlleva el uso de equipos portátiles; en la medida de lo posible, se deberá especificar equipos de escritorio para dichas adquisiciones.

Los Servidores Públicos, contratistas o terceros que tengan asignado un equipo portátil propiedad de la Gobernación deberán asegurarlo mediante una guaya de seguridad para su protección contra robo, en horas no laborables deberán almacenarse en lugares cerrados con llave. El código de seguridad de la guaya deberá ser entregado a la mesa de servicios una vez el portátil termine su uso en la ubicación que fue registrada en el inventario de activos de infraestructura de TI por el subproceso.

Es responsabilidad de los usuarios registrar el ingreso o salida de los equipos portátiles ya sean propios o de la entidad. Lo anterior, haciendo uso de los mecanismos aprobados por la Dirección de servicios administrativos y logísticos y dispuestos por la empresa de servicios de seguridad y vigilancia contratada.

Los equipos de escritorio, equipos de comunicación, impresoras y escáneres podrán ser trasladados fuera de las instalaciones o reubicados solamente con validación y autorización de la Dirección de sistemas de información después de un debido proceso de registro en el inventario de activos de infraestructura de TI por el subproceso administrador del activo.

El personal de seguridad y vigilancia de las instalaciones de la Gobernación tendrá la potestad de recoger y entregar al encargado de seguridad digital los equipos de propiedad de la Entidad (con placa oficial) que se encuentren sin su respectiva guaya de seguridad junto con un formato, definido por la empresa de vigilancia, que registre el suceso; esto en el caso de que el responsable del equipo se encuentre ausente.

Todos los equipos servidores y equipos de comunicaciones deberán estar ubicados en sitios con seguridad adecuada para protegerlos de usos no autorizados y posibles alteraciones.

Se deberá definir el procedimiento o los mecanismos para el soporte y mantenimiento a los equipos de cómputo, servidores y equipos activos de red, y llevar registro de estos.

Se deberá asegurar el soporte a los usuarios de los equipos de cómputo, asignados para el desarrollo de actividades, siempre y cuando los equipos sean de propiedad de la entidad. Las incidencias o solicitudes de soporte se atenderán cuando sean solicitadas a la mesa de servicios conforme al procedimiento definido para ello.

Cuando un equipo de cómputo sea reasignado o retirado de servicio (dado de baja), la Dirección de Sistemas de Información deberá garantizar la eliminación de toda información mediante mecanismos de borrado seguro teniendo en cuenta que previo a esta actividad el custodio o productor de la información le haya realizado una copia de seguridad.

Directriz de escritorio limpio y pantalla limpia

Con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo, en ausencia del personal acreditado, se ha establecido que no deben colocarse medios de almacenamiento (CDs, DVDs, cintas, memorias USB) ni documentos físicos sobre el escritorio o puesto de trabajo, estos deberán quedar bajo llave en gabinetes o en archivadores seguros.

Todos los equipos de cómputo, las impresoras y escáneres de la entidad se deberán apagar o poner en estado de suspensión cuando no estén en uso; además, se deberán retirar los documentos de las impresoras y no dejarlos sin protección.

Cuando el usuario se retira de su puesto de trabajo, se bloqueará o suspenderá el equipo (instrucción: + L). Los usuarios de equipos de cómputo estarán obligados a utilizar protector de pantalla protegido con contraseña para que el bloqueo sea automático después de unos minutos de inactividad del mismo (entre tres y cinco minutos es razonable).

Para todos los usuarios de las aplicaciones y sistemas de información de la Entidad, es obligatorio que las sesiones sean cerradas al finalizar las actividades y no se deben dejar abiertas o desatendidas.

POLÍTICA 7: USO DE CORREO ELECTRÓNICO Y OTROS SERVICIOS DE INTERNET EN TRABAJO COLABORATIVO

Para garantizar la integridad y confidencialidad de los servicios de correo electrónico, sus redes, instalaciones y datos, los funcionarios y demás usuarios que utilizan el servicio de correo electrónico institucional, servicios de correo de servidores gratuitos y de otros servicios de Internet para el trabajo colaborativo deben aceptar y cumplir los siguientes lineamientos:

El intercambio electrónico de información se realizará con base en estándares de documentos electrónicos y mensajes de datos de dominio público, regidas por organismos idóneos de carácter nacional e internacionales, y en algunos casos utilizando mecanismos criptográficos de clave pública y firma digital, especialmente en el caso de la información sensible. Para esta directriz se tendrá en consideración la ley 527 de 1999: "por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones."

Directriz de uso aceptable de los servicios

- Las comunicaciones oficiales por parte de los funcionarios públicos que requieren el uso de correo electrónico deben ser enviadas y recibidas a través de la dirección de correo electrónico institucional proporcionada por la Dirección de Sistemas de Información.
- El sistema de correo electrónico, el servicio de comunicación instantánea, y el servicio de Internet, deben ser usados únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades establecidas.
- El funcionario o tercero es responsable de todos los contenidos que se transmiten, reciben y almacenan a través del uso del cliente de servicio de correo electrónico; la Dirección de Sistemas de Información de la Gobernación de Boyacá no se hace responsable por el contenido almacenado en los buzones o por el contenido de paso en la red.
- El servicio de correo electrónico institucional se asignará o retirará según novedades reportadas por la Dirección General de Talento Humano.
- El servicio de correo electrónico institucional puede ser retirado a un funcionario o su cuenta bloqueada en cualquier momento, a discreción de la administración, si se observa un uso indebido o un alto porcentaje de recepción de mensajes spam.
- Cuando se envíe un correo electrónico a múltiples destinatarios, se deberá ocultar los destinatarios utilizando el apartado CCO (con copia oculta) para evitar la revelación de sus direcciones, especialmente cuando va dirigido a ciudadanos o personas externas. Así mismo, se deberá ingresar las direcciones de correo institucional a la lista de contactos.
- Los Directivos solicitarán la creación, reinicio o cancelación de las cuentas electrónicas diferentes a los asignados a la dependencia, según funciones asignadas.
- Para la creación de correos electrónicos a personal contratista los directivos solicitarán la creación solo para programas o proyectos que requieran envíos oficiales y la denominación del correo electrónico no corresponderá a nombres personales sino al tema específico así: nombretema.dependencia@boyaca.gov.co.
- Cada cuenta de correo electrónico institucional asignada al funcionario deberá tener identificado al servidor público responsable así: primernombre.primerapellido@boyaca.gov.co, en caso de presentarse homónimos se revisará el caso particular. Las secretarias y direcciones se identificarán con el nombre de la dependencia tanto para el directivo como para el despacho de la misma, de la siguiente manera: para directivos secretario.nombredependencia@boyaca.gov.co , para despachos: despacho.nombredependencia@boyaca.gov.co.
- Las cuentas de correo electrónico y sus copias de seguridad son propiedad de la Gobernación de Boyacá y quienes tengan asignado éste servicio deben utilizarlo única y exclusivamente para las tareas propias de la función desarrollada en la Entidad; estas pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control.

- Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo a los niveles de importancia o de confidencialidad, para los cuales se requiere que sea etiquetado según necesidad como: Personal, Privado o Confidencial.
- El tamaño del buzón de correo electrónico se asigna de manera estandarizada, la capacidad específica es definida y administrada por la Dirección de Sistemas de Información.
- Periódicamente el administrador de cuentas revisará las cuentas que llevan más de 60 días sin ningún acceso. En caso tal, las cuentas diferentes a las asignadas a la dependencia que corresponden a programas o eventos, se procederá a enviar una comunicación de dichas cuentas sin uso advirtiendo del proceso de eliminación y se darán 30 días adicionales a partir de la fecha de la comunicación para la utilización de las cuentas. Vencidos los 30 días, de no presentarse uso o de no haber recibido justificación de necesidad de uso, se procederá a la eliminación y se entenderá que el usuario ya ha sido comunicado y que la cuenta no es necesaria. Para el caso de funcionarios de planta con cuentas de correo sin uso se reportarán a la Oficina de Control Interno de Gestión trimestralmente para dejar precedente.
- Cuando un funcionario, al que le haya sido autorizado el uso de una cuenta de correo electrónico, se retire de la entidad su cuenta de correo será bloqueada y con restricción de recepción de mensajes.
- Las cuentas de correos que permanezcan con estado bloqueado se conservarán por el término de un (1) año, después de ese lapso de tiempo se realizará el proceso de eliminación.
- Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido, ya que pudieran ser mensajes de spam y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. Por lo que se debe marcar el mensaje como correo no deseado, bloquear al remitente en opciones de seguridad y proceder a eliminar el mensaje del correo para no recibir futuros mensajes de él.
- Revisar la bandeja de "Correo no deseado" o de spam, a fin de encontrar posibles mensajes válidos o seguros identificados como spam y deben ser movidos a la bandeja de entrada aplicando la opción de "*No es un correo no deseado*" y para que en adelante se reciba en la bandeja de entrada se debe agregar a los remitentes seguros.
- Se podrá adoptar para aquellos casos que se requiera de un correo electrónico temporal o transitorio, la configuración de alias o seudónimos asociados a un buzón existente, permitiendo de ésta manera recibir mensajes en un solo buzón para diferentes direcciones de correo adicionales, por ejemplo direccion.dependencia@boyaca.gov.co como dirección de correo principal se podrá asignar otros nombres adicionales como convocatoria.dependencia@boyaca.gov.co o proyectos.dependencia@boyaca.gov.co y se aplicarían reglas para separar los mensajes dentro del mismo correo; sin embargo, los correos que se envíen (salientes) desde esa dirección, tendrán como remitente la dirección del correo electrónico principal. Al crear un alias, este no contará como una nueva cuenta de correo, sino que será una forma distinta de llamar a la misma cuenta.
- Cuando un mensaje es identificado como altamente inseguro y no llega a ninguna de las bandejas del buzón, es probable que se encuentra en estado "*Cuarentena*" y el remitente fue identificado como inseguro, por tanto, deberá buscar su correo en Configuración->Correo-> Correo electrónico no deseado y en la lista de correos bloqueados, eliminarlo y agregarlo a la lista de remitentes seguros y solicitar a la Dirección de Sistemas liberar los mensajes bloqueados del remitente identificado.
- La información almacenada en los archivos de tipo .PST es responsabilidad de cada uno de los usuarios y cada usuario debe realizar la depuración periódica del buzón para evitar que alcance su límite.
- Es responsabilidad del usuario depurar los grupos de trabajo o las listas de distribución.
- Los correos electrónicos deben contener la siguiente nota de confidencialidad respecto al manejo del contenido así:
  "El contenido de este mensaje y sus anexos son propiedad de la Gobernación de Boyacá, es únicamente para el uso del destinatario ya que puede contener información pública reservada o información pública clasificada (privada o semiprivada), las cuales no son de carácter público. Si usted no es el destinatario, se informa que cualquier uso, difusión, distribución o copiado de esta comunicación está prohibido. Cualquier revisión, retransmisión, diseminación o uso del mismo, así como cualquier acción que se tome respecto a la información contenida, por personas o

entidades diferentes al propósito original de la misma, es ilegal. Si usted es el destinatario, le solicitamos dar un manejo adecuado a la información; de presentarse cualquier suceso anómalo, por favor informarlo al correo seguridad.digital@boyaca.gov.co".

- La clave o contraseña de acceso que se defina por el usuario de correo electrónico deberá cumplir con la Directriz de contraseñas para acceso a la información y a las aplicaciones definida en la política de control de acceso del presente documento.
- Todos los usuarios de correo electrónico institucional por estándar tendrán configurado un tamaño máximo para recibir o enviar mensajes de 35 MB (incluyendo la suma de todos los adjuntos) y un límite de destinatarios de 500.
- Las carpetas compartidas sobre la infraestructura ofrecida por la Gobernación de Boyacá de otros servicios como: SharePoint y OneDrive, serán administradas por las dependencias quienes velarán por el buen uso de la información y de las carpetas.
- Es responsabilidad del usuario permitir los accesos a las carpetas compartidas, usando los criterios de acceso de lectura, escritura y control total. Configuración para usuarios externos: 1) Cualquier persona que tenga el vínculo, 2) Personas determinadas (Preferible); Configuración para usuarios internos: 1) Usuarios de Gobernación de Boyacá que tengan el vínculo, 2) Personas que tienen el acceso.
- El servicio de chat o mensajería instantánea para la comunicación interna, que maneje el personal, deberá dar utilidad a la herramienta definida de acuerdo a los servicios oficiales contratados para trabajo colaborativo, o en su defecto la herramienta definida por el Jefe inmediato o supervisor, siempre dando cumplimiento a directrices de privacidad y confidencialidad de la información durante la transferencia de mensajes.

Directriz del uso no aceptable de los servicios

- Las comunicaciones oficiales por parte de los funcionarios públicos que requieren el uso de correo electrónico no deben realizarse mediante cuentas personales de correo electrónico.
- No se deben enviar mensajes tipo spam que son excesivos y/o destinados a acosar o molestar a los demás ya que afecta gravemente la eficiencia y costo-beneficio del servicio.
- Los servicios de correo electrónico solo podrán utilizarse con fines lícitos, no deben utilizarse para otro fin; no se debe constituir marketing engañoso, o para el desarrollo de actividades políticas, comerciales no se debe mantener contenido obsceno, ofensivo, racista, difamatorio, abusivo, o fraudulento.
- No se deben enviar mensajes de correo electrónico en donde el destinatario sea el grupo de todos los funcionarios, salvo que sea un asunto oficial de la alta dirección que involucre a toda la Entidad o que no amerite circular por el Sistema de Gestión Documental.
- En casos donde se recibe spam no se debe contestar dichos mensajes, no entregar datos personales, ni información financiera, ni abrir los archivos adjuntos y en tal caso reenviar el correo sospechoso a la cuenta seguridad.digital@boyaca.gov.co con la frase "correo sospechoso" en el asunto.
- No violar los términos de uso del servicio de correo electrónico definidos por el proveedor, lo que se puede consultar en el sitio web oficial del mismo, en el documento contrato de servicios.
- No se debe realizar ninguna acción destinada a manipular la identidad del usuario o la información de contacto, que omita, elimine, falsifique o tergiverse la información contenida en los mensajes.
- Los funcionarios públicos, contratistas y demás usuarios no deben utilizar versiones escaneadas de firmas hechas a mano para aparentar que un mensaje de correo o cualquier otro tipo de comunicación electrónica fue firmado por el remitente. Se debe utilizar una firma estándar de texto que se compone de nombres y apellidos, cargo, dependencia y número de teléfono.
- No abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.

- La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de compras, deportivas, almacenes de cadena, plataformas de pago, compras en línea, juegos, casinos, páginas de pornografía o en cualquier otra página ajena a los fines de la entidad.

POLÍTICA 8: SEGURIDAD EN TELECOMUNICACIONES Y SERVICIOS ASOCIADOS

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser consideradas y tratadas como información sensible.

La red de cobertura geográfica local debe estar dividida en forma lógica por diferentes segmentos de red, cada uno separado con controles de seguridad perimetral y mecanismos de control de acceso, a través del Firewall.

Todas las conexiones de redes externas de tiempo real que accedan a la red interna, deberán pasar a través del sistema de defensa electrónica con tecnologías: Sistema de Prevención de Intrusos (IPS), Firewall, Filtro de contenido o de Red Privada Virtual (VPN), anti-virus y anti-spyware, y de control de aplicaciones.

La Entidad deberá asegurar la protección de las redes y la trasferencia de información, e implementar controles de monitoreo de la red.

Los servidores de aplicaciones y servidores Web internos tendrán configuraciones para la protección de tráfico, en cuanto a amenazas ocultas, con tecnologías como la de cifrado SSL.

Se deberá hacer el bloqueo a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso institucional, mediante el uso de servidor proxy, firewall o control que mejor se ajuste a la necesidad. El servicio de acceso a Internet se deberá prestar con restricciones de acuerdo a políticas de Firewall definidas para proporcionar una conectividad confiable y controlar ataques informáticos por la red, phishing y fuentes de software malicioso (malware).

El servicio de acceso a Internet puede ser retirado en cualquier momento, a discreción de la Administración, si se observa un uso indebido o un bajo rendimiento del Servidor, para dar espacio a procesos que tengan mayor prioridad o mayor relevancia.

La transferencia de información deberá realizarse protegiendo la confidencialidad, integridad y disponibilidad de los datos de acuerdo con la clasificación del activo y el tipo información involucrada.

Los funcionarios públicos se obligan a NO utilizar la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras, impresoras, o cualquier equipo que genere caída de la energía. Esos equipos eléctricos, si están autorizados, se podrán conectar a la red no regulada de energía.

Las áreas de la Entidad que estén destinadas a realizar en su operación transacciones financieras deberán dar cumplimiento a los lineamientos establecidos por el MinTIC, para el aseguramiento de los equipos o terminales móviles.

POLÍTICA 9: TELETRABAJO Y TRABAJO EN CASA

Los lineamientos de esta política se definen dentro del marco normativo que establecen la ley 1221 de 2008 que regula el Teletrabajo y la ley 2088 de 2021 que regula el Trabajo en casa; también atendiendo a las políticas relacionadas de este manual.

Toda información gestionada por la Entidad, a la cual tiene derecho de acceso el trabajador y la que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales dando cumplimiento a directrices de privacidad y confidencialidad de la información mencionada en este documento.

Se deberá garantizar a través de capacitaciones el uso adecuado de las tecnologías de la información y la comunicación (TIC) especialmente de las herramientas colaborativas para el trabajo remoto en equipo. La capacitación y el desarrollo de competencias digitales que hagan parte del programa institucional de capacitación se reforzarán para los trabajadores que inicien la modalidad o habilitación del trabajo remoto.

La Entidad establece los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos y compromisos de contratistas de la entidad, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de la información con los servicios que se habiliten por este canal.

Para acceder a los servicios por conexión remota, dado que es un canal ocasional, se deberá tener visto bueno del director o secretario del área solicitante y la validación por parte de la Dirección de Sistemas de Información. Entonces, se creará una conexión de red privada virtual (VPN) para que el funcionario solicitante pueda conectarse remotamente a la red de la Gobernación para acceder a sistemas de información y otros servicios a que tenga acceso.

El trabajador deberá custodiar los activos de TI o activos de información y retener copia de la información que se produzca en el ejercicio de sus funciones dando cumplimiento a la política de gestión de activos de información y a la política copias de seguridad de archivo electrónico y retención definida en este documento.

Una vez cese la modalidad de trabajo remoto y se reanude la presencialidad del trabajador en la Entidad, se deberá retornar la información producida de manera organizada, evitando la impresión en papel a menos que sea estrictamente necesario para algunos archivos, organizando y almacenando los documentos electrónicos de archivo y bases de datos conforme a la política de clasificación y ordenación de la información señalada en este documento.

En todo caso, los servidores públicos y contratistas deben hacer la devolución de los activos de información asignados a su cargo ya sea que finalice la relación contractual con la Entidad, la habilitación de trabajo en casa o la modalidad de teletrabajo.

Directriz de lineamientos técnicos para habilitación de trabajo en casa

Además de lo ya señalado en esta política, para la habilitación del trabajo en casa se deberá tener en cuenta lo siguiente:

- Se dará privilegio al uso de tecnologías de la información y las comunicaciones en cualquier tipo de trabajo o labor que no requiera la presencia física del trabajador o funcionario en las instalaciones de la entidad, según indicaciones en la Ley 2088 de 2021, cuando se presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus funciones en su lugar de trabajo.
- Se deberá fijar los medios y herramientas que permitan el reporte, seguimiento y evaluación, así como la comunicación constante y recíproca entre el jefe directo y el trabajador con el fin de dar cumplimiento a los objetivos y actividades obedeciendo a criterios concertados y establecidos con anterioridad. Así mismo, se deberá disponer

de equipo, conexión remota a red privada virtual (VPN), sistemas de información e información para el desarrollo de la función o labor desde casa, de acuerdo a los recursos disponibles.

- Se deberá dar a conocer a los ciudadanos y usuarios de los servicios virtuales los canales oficiales de comunicación e información mediante los cuales se prestarán los servicios de manera virtual, así como los mecanismos tecnológicos y/o virtuales que se emplearán para el registro y respuesta de las peticiones.

Directriz de lineamientos técnicos para modalidad de teletrabajo

Además de lo ya señalado en la introducción de esta política, los funcionarios públicos que se postulen, sean asignados en modalidad de teletrabajo y permanezcan en esa modalidad por un determinado período de tiempo, deberán:

- Contar con el certificado del curso de Seguridad y privacidad de la información establecido ya sea por la Secretaría de TIC y Gobierno abierto o por el MinTIC.
- Haber asistido a la socialización sobre políticas de seguridad digital programada por la Dirección de sistemas de información.
- Demostrar uso permanente por parte del Teletrabajador del Servicio de Correo electrónico institucional (se verifica con informe o estadísticas tomadas de la respectiva plataforma en el último trimestre).
- Demostrar uso permanente del Servicio de herramientas colaborativas oficiales para trabajo en equipo (se verifica con informe o estadísticas tomadas de la respectiva plataforma en el último trimestre).
- Dar aplicabilidad a los requisitos de elementos y características técnicas y tecnológicas mínimas exigidas en el respectivo anexo técnico que haga parte la modalidad de teletrabajo.

Se deberá asegurar el soporte a los usuarios Teletrabajadores sobre los equipos de cómputo aprobados para el desarrollo de actividades; así mismo, se garantizará el soporte sobre los servicios que estén incluidos en el catálogo de servicios tecnológicos y los sistemas de información que administre la Dirección de Sistemas de información.

POLÍTICA 10: SEGURIDAD DE LOS RECURSOS HUMANOS

La Secretaría de Contratación y quienes lideren el proceso de contratación de personal en la Entidad deben realizar las verificaciones de los antecedentes (procuraduría, contraloría, policía) de los candidatos a un cargo, la formación académica, experiencia y demás información que se requiera, de acuerdo a las leyes, reglamentos de la Entidad, transparencia y ética pertinente.

La Entidad debe incorporar los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los Colaboradores y Terceros. Los deberes de los servidores públicos y los acuerdos contractuales entre la Entidad y los contratistas especificarán el cumplimiento a los lineamientos de seguridad de la información establecidos en la Entidad, a través de este documento, especialmente los establecidos en las directrices de privacidad y confidencialidad de la información.

La Entidad establece la directriz para asegurar que los servidores públicos y contratistas tengan conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad de la información. Por lo anterior, todo servidor público y contratista debe recibir inducción y procesos periódicos de sensibilización en seguridad y privacidad de la información en la Entidad, a partir de las estrategias y programas definidos para ello.

La Dirección General de Talento Humano y la Secretaría de Contratación deben establecer mecanismos y controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.

La Dirección General de Talento Humano y la Secretaría de Contratación deben realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los servidores públicos y de compromisos de los contratistas llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin; Así mismo, los directores, jefes, supervisores de contrato o líderes deben informar la desvinculación, cambio de labores o de compromisos de acuerdo con los procedimientos; dicha información debe ser entregada oportunamente al proceso de Gestión de TI, y en atención a la política descrita denominada “Control de acceso a la información y a las aplicaciones”.

La Entidad efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará a la Secretaria de TIC y Gobierno Abierto los casos de incumplimiento con copia a la Oficina asesora de Control interno de gestión; esta última escalará a la Oficina asesora de Control interno disciplinario o a entes de control de ser necesario.

En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se deberá tramitar el cumplimiento de la ley 734 de 2013 Código disciplinario único, Leyes 1437 de 2011 y 2080 de 2021 Código de procedimiento administrativo y de lo contencioso administrativo. Así como, el cumplimiento de la Ley 1474 de 2011 Estatuto anticorrupción y demás normas que reglamenten los procesos disciplinarios para los empleados del estado y el control fiscal sobre contratación pública.

POLÍTICA 11: SEGURIDAD PARA USUARIOS TERCEROS / PROVEEDORES

Se deben establecer y aplicar criterios de selección que contemplen la experiencia y reputación de proveedores o contratistas por tercerización de servicios (outsourcing), certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad, y otros criterios que resulten de un análisis de riesgos en la etapa precontractual.

Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de la Gobernación de Boyacá, las cuales deben ser divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

Los proveedores o contratistas por outsourcing deben aceptar y firmar el acuerdo de confidencialidad establecido para la protección de la información y los datos personales, así como el compromiso del cumplimiento de las políticas de seguridad y privacidad de la información de la Gobernación de Boyacá, ya sea en un documento anexo al contrato o dentro de las cláusulas del mismo.

Los proveedores o terceros deberán realizar el análisis y gestión de riesgos tanto de la labor o proyecto contratado como de la información y otros activos de información que hacen parte del flujo o intercambio entre las partes.

Los usuarios proveedores o terceros, tendrán acceso a los servicios tecnológicos, que sean estrictamente necesarios para el cumplimiento de sus compromisos y labor; solicitudes de acceso que deben ser aprobadas por quien sea Interventor / Supervisor, o Directivo del proceso o subproceso involucrado y enviadas a la Dirección de Sistemas de información conforme se indica en la política de control de acceso establecida en este documento.

La conexión entre sistemas de información internos y otros de terceros, debe ser aprobada por la Dirección de Sistemas de Información con el fin de no comprometer la seguridad de la información interna de la entidad.

Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad informática vigentes en la Entidad y deben estar registrados ante la Dirección de Sistemas de Información.

Como requisito para interconectar las redes de la entidad con las de terceros, los sistemas de comunicación o de conexión de terceros deben cumplir con las políticas de seguridad establecidas por la Gobernación de Boyacá. Esta última se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La entidad se reserva el derecho de cerrar o inactivar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos.

El personal no deberá suministrar información de la entidad a ningún ente externo sin las autorizaciones respectivas de la dependencia que custodia la información. Especialmente, se deberá tener atento cumplimiento a directrices de privacidad y confidencialidad de la información.

Los proveedores o terceros que sean autorizados para ingresar a las redes o a los Sistemas de Información de la Gobernación de Boyacá, solamente pueden tener privilegios de acceso a los recursos informáticos durante el periodo de tiempo necesario determinado para llevar a cabo los compromisos o labores a su cargo.

Para proveedores de tecnologías de Información valorada como crítica, así como de procesos misionales; la Entidad exige que se cuente con planes de continuidad de negocio y recuperación de desastres definidos e implementados, de modo que proveedores contratados puedan responder ante eventuales escenarios que afecten el suministro de servicios o productos a la Entidad.

Los proveedores de tecnologías de información deben dar cumplimiento a los Acuerdos de Nivel de Servicio (ANS) establecidos en el proceso de contratación, los cuales serán verificados periódicamente por la Dirección de sistemas de información.

POLÍTICA 12: PROPIEDAD INTELECTUAL Y ADMINISTRACIÓN DE LICENCIAS DE SOFTWARE

La propiedad intelectual de los avances tecnológicos e intelectuales, derivados del objeto de cumplimiento de funciones, tareas asignadas y de compromisos contractuales, desarrollados mientras el trabajador, funcionario o contratista se encuentre prestando servicios para la Entidad, es propiedad exclusiva de la Gobernación de Boyacá.

Esta política incluye invenciones, patentes, derechos de reproducción, marca registrada, dibujos y modelos industriales, indicaciones geográficas de origen, obras literarias y artísticas, fonogramas, programas de radio y televisión, y otros derechos de propiedad intelectual según lo manifestado en planes, estrategias, productos, programas de aplicación, documentación y otros materiales.

La Gobernación de Boyacá es propietaria de los activos de información que identifican y declaran los procesos y subprocesos de la entidad; los administradores de estos activos son los funcionarios, contratistas o demás colaboradores denominados “Usuarios” que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura tecnológica.

Se debe propender a una cultura informática al interior de la Gobernación de Boyacá que garantice el conocimiento por parte de los funcionarios públicos, contratistas y demás usuarios acerca de las implicaciones que tiene el instalar y usar software ilegal en los computadores de la entidad, teniendo en cuenta, además que únicamente los funcionarios de la Dirección de Sistemas de Información están autorizados para realizar cambios en el software de los equipos oficiales.

Todo software que utilice la Gobernación de Boyacá será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos o reglamentos internos de contratación, además del visto bueno técnico por parte de la Dirección de Sistemas de Información.

Deberá existir un inventario de las licencias de software de la Gobernación de Boyacá que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

Los productos de software con licencia de evaluación o de prueba instalados en los computadores de la Gobernación de Boyacá deberá desinstalarse una vez caduque la licencia.

La instalación de software debe ser autorizada y realizada por funcionarios de la Dirección de Sistemas de Información. Los funcionarios públicos, contratistas y demás usuarios no deben instalar ningún tipo de software; el software pirata, ilegal o material digital que viole las normas de seguridad y de derechos de autor será desinstalado o eliminado.

POLÍTICA 13: ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La Entidad asegura que se diseñe e implemente los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.

La Entidad establece controles técnicos para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información que son públicos mediante herramientas de seguridad perimetral de proveedores o de forma local.

Los sistemas de información de la Entidad deberán contar con un ambiente de desarrollo y de pruebas seguro o, en su defecto, se exigirá al proveedor mediante los contratos, que éste cuente con los controles de seguridad de la información sobre dichos ambientes.

Todos los sistemas de información o software desarrollado deben tener asignado un administrador, dentro del área funcional o del área técnica según sea el caso, que sea responsable de la administración y custodia dentro de la Gobernación.

Antes que un nuevo sistema de información se desarrolle o se adquiera por parte de la Gobernación de Boyacá, la mesa técnica de Gobierno y Seguridad digital deberá avalar las especificaciones y requerimientos de seguridad necesarios para su implementación.
La seguridad en el acceso a las aplicaciones debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño o de arquitectura de sistemas hasta la conversión a un sistema en producción.

Como se ha indicado en la política de seguridad para usuarios terceros, los proveedores de tecnologías de información deben dar cumplimiento a los Acuerdos de Nivel de Servicio (ANS) establecidos en el proceso de contratación, los cuales serán verificados periódicamente por la Dirección de sistemas de información.

Los ANS para los sistemas de información deberán considerar los requerimientos de seguridad de la información, interoperabilidad y apertura de datos establecidos en la política nacional de Gobierno digital; así mismo, teniendo en cuenta aspectos de estandarización, arquitectura de sistemas, metodologías ágiles y otros citados en las mejores prácticas.

Se deberá exigir a los proveedores de sistemas de información toda la documentación de los repositorios, bases de datos, arquitectura del sistema, manuales de instalación y manuales de usuario final.

POLÍTICA 14: ADMINISTRACIÓN DE CAMBIOS

Para realizar cambios de las Tecnologías de Información y Comunicación se efectuará el procedimiento correspondiente definido por la Dirección de Sistemas de Información, que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos, para garantizar estándares de eficiencia, seguridad, calidad y que permitan determinar los responsables y tareas a seguir para garantizar el éxito en los cambios.

Se deberá definir un procedimiento o instructivo que señale responsabilidades y tareas relacionadas con el cambio (creación, modificación, o eliminación de interfaces y reportes) que se necesite en las aplicaciones informáticas. Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por el usuario, o un tercero externo que no haya sido contratado para ese propósito.

Cualquier cambio que se requiera en los equipos de cómputo de la Gobernación de Boyacá (repotenciación o reparación) se debe evaluar técnicamente y ser autorizado. La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal de la Dirección de Sistemas de Información, y se registrará el cambio de repuesto o reparación ya sea en la hoja de vida del equipo o en el sistema de mesa de servicios.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de manera acorde a los requisitos de seguridad existentes y autorizados por la Dirección de Sistemas de Información.

Cualquier tipo de cambio en la plataforma tecnológica debe ser documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

Los cambios en recursos tecnológicos que sean implementados deberán desarrollar la estrategia de uso y apropiación que se tenga definida, aplicada según la necesidad, para garantizar que los usuarios procedan con conocimiento en el manejo de las nuevas herramientas o nuevas funcionalidades derivadas de las ya existentes.

POLÍTICA 15: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Los usuarios de tecnologías y sistemas de información deberán comunicar de manera oportuna los incidentes de seguridad ocurridos, a través de los diferentes canales dispuestos para tal fin, a la Dirección de Sistemas de Información: mesa de servicios y correo electrónico seguridad.digital@boyaca.gov.co.

Se debe dar tratamiento adecuado a los incidentes de seguridad de la información reportados; los que no puedan resolverse de forma inmediata serán escalados apropiadamente de acuerdo al procedimiento o instructivo establecido para ello con el propósito de tomar acciones efectivas para minimizar el impacto.

Para gestionar los incidentes de Seguridad de la Información deberá existir un Grupo técnico de Gestión de riesgos de Seguridad digital con conocimientos en el manejo de incidentes ocurridos en las áreas de Seguridad de la Información; quienes deberán llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos, donde se detalle la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.

La Entidad debe asegurarse que todos los servidores públicos y contratistas conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información, a través del programa de sensibilización y formación sobre seguridad de la información.

Los incidentes de seguridad que evidencien violaciones a las políticas de seguridad de la información tendrán el curso señalado en la Política de administración de la seguridad definida en este documento.

Una vez verificada por la Dirección de Sistemas de Información y la Oficina asesora de Control Interno de Gestión la existencia de un incidente crítico que involucre a un funcionario, el cual incurra en incumplimientos o faltas que ameriten sanción disciplinaria sin perjuicio de la ley, se escalará a la Oficina Asesora de Control Interno Disciplinario para que se coordine y determine el alcance a las investigaciones según sea el caso.

Para cuando los incidentes reportados requieran judicialización se deberá coordinar con el/ los organismos que cuentan con función de policía judicial. Se deberá establecer los mecanismos de control establecidos en el manual de procedimientos del Sistema para Cadena de Custodia de la Fiscalía General de la Nación para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de Seguridad de la Información.

POLITICA 16: SEGURIDAD EN LAS OPERACIONES

La Entidad debe documentar los procesos operacionales (instructivos, manuales) a nivel de TI, para reducir riesgos asociados con pérdida de la información y afectaciones en la infraestructura tecnológica.

La Entidad debe garantizar que las operaciones Tecnológicas se desarrollen en un ambiente controlado y se brinde seguridad a las áreas de procesamiento de información.

Se debe contar con herramientas de protección tales como antivirus, antimalware, anti spam y antispyware que reduzcan el riesgo de contagio de software malicioso en los equipos propios de la entidad, usando una consola de antivirus.

Se debe asegurar que el software de antivirus, antimalware, antispyware y anti spam cuente con las licencias de uso requeridas, y posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Se deberá aplicar los parches, controles o remediaciones derivadas de la ejecución de pruebas periódicas de análisis de vulnerabilidades.

Según la clasificación de la información definida por los procesos y subprocesos de la Entidad, se deberán establecer las medidas de respaldo de la información a través de mecanismos como unidades de cintas, discos de almacenamiento o en la nube.

Se deberá gestionar la capacidad de la Infraestructura tecnológica en cuanto a procesamiento, almacenamiento y servicios de red realizando proyecciones de crecimiento y el aprovisionamiento necesario para la optimización y disponibilidad de los servicios tecnológicos y sistemas de información de la Entidad.

En el desarrollo de plataformas, servicios de información o sistemas de información ya sea a nivel interno o contratado a terceros se deberá separar ambientes de pruebas de los de producción; todo cambio que se deba realizar en ambientes de producción deberán ser experimentados y examinados previamente en ambientes de pruebas.

POLÍTICA 17: CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESATRES

Directriz de continuidad del negocio

- Se debe elaborar y aprobar la planeación de Continuidad de servicios de TI y recuperación de desastres, que incorpore estrategias para el cumplimiento de las políticas de continuidad y recuperación, documentado en el plan de seguridad y privacidad de la información.
- Se debe realizar mejoras a la planeación de continuidad de forma periódica o ante cambios significativos tales como procesos, tecnología o estructura organizativa; para lo cual deberán participar activamente en dicha revisión las distintas áreas de los procesos identificados como críticos.
- Los custodios y administradores de la información en cada una de los subprocesos de las Sectoriales deben identificar, clasificar y priorizar la información crítica de sus procesos.
- Los custodios y administradores de los sistemas de información deben identificar y priorizar aplicaciones de software, que se encuentren operando en cada una de las sectoriales.
- Los procesos y subprocesos de la Entidad deben realizar el análisis y gestión de riesgos de continuidad del negocio y hacer el tratamiento que corresponda, conforme al proceso y política general de Administración del Riesgo en la Entidad.
- Se debe establecer un Análisis de impacto al negocio (BIA) por medio del cual se identifiquen los servicios y activos de información críticos de la Gobernación conforme a la priorización realizada previamente; así mismo, en el que se identifiquen los incidentes disruptivos y su impacto, incluyendo el escenario por pandemia.
- Se debe establecer el tiempo aceptable para recuperar los datos que tiene la Entidad en caso de una interrupción o desastre (RPO), y garantizar una recuperación eficaz.
- Se debe establecer el tiempo para retornar a las actividades normales después de la interrupción o desastre (RTO), y garantizar que los procesos críticos son recuperados dentro de los márgenes de tiempo requeridos en el Plan de Continuidad.
- La estrategia de continuidad de servicios de Tecnologías de Información y recuperación de la Gobernación de Boyacá deberá diseñar e implementar actividades de prevención y de recuperación que ofrezcan las garantías necesarias para el restablecimiento de las operaciones de la Entidad después de un desastre. El análisis del impacto del negocio constituirá el punto de partida para la formulación de las estrategias.
- Se debe contar con equipos servidores alternos, ya sea locales o infraestructura en la nube, que permitan tener disponibles versiones de sistema operativo, plataformas de base de datos, de servicios Web y configuraciones necesarias que estén compatibles y sincronizados con los servidores principales.
- Se debe disponer de energía eléctrica a través de Sistemas de Alimentación Ininterrumpida y plantas eléctricas para suministrar energía a los equipos de cómputo, principalmente a equipos servidores.
- Se debe garantizar la divulgación y concientización de las políticas y de la planeación de Continuidad de servicios de TI y recuperación de desastres dentro de la cultura de la Gobernación de Boyacá.

Directriz de recuperación de servicios TI por desastre

- Se debe contar con una ubicación física desde la cual el plan de recuperación de desastres pueda ser ejecutado; es decir, un centro de procesamiento alterno con capacidad para el respaldo de las operaciones críticas de la Entidad.
- Se debe contar con una estrategia de habilitación de trabajo en casa y/o de teletrabajo para caso de incidente disruptivo como el de escenario de pandemia, donde los trabajadores no pueden hacer uso de todos los recursos tecnológicos ubicados en las instalaciones de la Entidad. Lo anterior, dando cumplimiento a política de teletrabajo y trabajo en casa definida en este documento.
- Se deberá establecer un protocolo de activación del plan y notificación oficial en la Gobernación de Boyacá ante la ocurrencia de un desastre. Una vez que la notificación se ha hecho, los responsables deberán activar al personal apropiado para realizar las actividades de verificación y evaluación.
- Se deberá realizar la verificación del desastre y evaluación de daños. Una vez que la evaluación se ha hecho, los responsables deberán activar al personal apropiado para realizar las actividades de soporte y recuperación.
- Se debe realizar copia de seguridad (Backup) de las aplicaciones, bases de datos y bodegas de archivos alojados en servidores, con el propósito de salvaguardar la información. Estas se deben realizar periódicamente por profesionales de la Dirección de Sistemas de Información, de acuerdo a las indicaciones establecidas en el plan de continuidad y se deberán almacenar en un sitio alterno fuera del edificio donde se encuentra en centro de procesamiento principal.
- Se debe realizar copias de seguridad (Backup) de la información más relevante almacenada en equipos cliente en cada una de las dependencias, esta debe ser ejecutada por el funcionario (administrador de la información) de la dependencia.
- Se deben almacenar las copias de seguridad de archivos relevantes de las dependencias, organizadas en archivos electrónicos de documentos, incluyendo sus metadatos a través de Tablas de Retención Documental (TRD) y preservar los documentos según se indique en la TRD de cada dependencia.
- Se debe etiquetar los medios de almacenamiento con el propósito de identificar las características de la copia de seguridad, de acuerdo a las indicaciones definidas en el plan de Continuidad de servicios de TI y recuperación de desastres
- Los proveedores de Servicios de Tecnología de Información deben tener capacidad para brindar soporte a requerimientos que se deriven después del desastre.

POLÍTICA 18: ADMINISTRACIÓN DE LA SEGURIDAD

La evaluación de riesgos de seguridad para los Recursos Informáticos en producción se debe ejecutar al menos una vez cada año. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.

Los funcionarios públicos y contratistas de la Gobernación de Boyacá que realizan las labores de administración del recurso informático y de servicios son responsables por la implementación, permanencia y monitoreo de los controles sobre los recursos computacionales. La implementación debe ser consistente con las prácticas establecidas por la Dirección de Sistemas de Información.

La Dirección de Sistemas de Información divulgará, las políticas, estándares y procedimientos en materia de seguridad digital a través de un Programa de sensibilización y formación en seguridad de la información.

Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar a los usuarios que lo requieran, de acuerdo con su competencia según las actividades a desarrollar y los niveles de seguridad establecidos previamente.

La Entidad efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará a la Secretaria de TIC y Gobierno Abierto los casos de incumplimiento con copia a la Oficina asesora de Control interno de gestión; esta última escalará a la Oficina asesora de Control interno disciplinario o a entes de control de ser necesario.

En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se deberá tramitar el cumplimiento de la ley 734 de 2013 Código disciplinario único, Leyes 1437 de 2011 y 2080 de 2021 Código de procedimiento administrativo y de lo contencioso administrativo. Así como, el cumplimiento de la Ley 1474 de 2011 Estatuto anticorrupción y demás normas que reglamenten los procesos disciplinarios para los empleados del estado y el control fiscal sobre contratación pública.

Directriz de Registros de auditoría

Todos los sistemas informáticos que operen y administren información sensible, valiosa o crítica para la Gobernación de Boyacá, como son sistemas de aplicación en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones deberán generar pistas de auditoría o logs de registro de sucesos de la operación, las cuales deben proporcionar suficiente información para apoyar el monitoreo, control y las mismas auditorias.

Todos los archivos de logs de auditorías deben ser almacenados y custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que con razón justificada y autorizada por la sectorial correspondiente requieran los registros deberán solicitarlos ante dicha dependencia, quien a su vez deberá solicitar el soporte adecuado a la Dirección de Sistemas de Información, encargada de su administración y custodia.

Todos los computadores de la Entidad deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoria y en las transacciones sea correcto. El servidor de dominio deberá tener sincronizada la hora con servidores de hora de Windows o similares para que los equipos que estén configurados en el dominio también se sincronicen correctamente.

No se permite la instalación, ni utilización de cualquier herramienta de auditoría ni de pruebas de seguridad informática, ni de Ethical Hacking sin previa autorización de la Dirección de Sistemas de Información.

Directriz de Derechos de vigilancia

- La Administración se reserva el derecho de supervisar e inspeccionar los sistemas de información de la entidad en cualquier momento.
- Estas inspecciones pueden llevarse a cabo con o sin el consentimiento y/o la presencia de los empleados involucrados.
- Los sistemas de información que pueden ser objeto de inspección incluyen el registro de actividad de los usuarios, los archivos del disco duro y correo electrónico.
- La entidad se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico. Para este efecto, el funcionario o contratista autoriza a la entidad para realizar las revisiones y/o auditorías internas o a través de terceros.

- También pueden estar sujetos a inspección los documentos impresos, cajones del escritorio y áreas de almacenamiento de medios.
- La Inspecciones sólo pueden realizarse después de haber obtenido la aprobación de la Oficina Asesora de Control Interno Disciplinario.
- La Administración se reserva el derecho de confiscar cualquier material ofensivo o información ilícita.
- La Administración se reserva el derecho a la monitorización de actividad en base de datos (Database Activity Monitoring - DAM) en tiempo real o casi real, incluyendo actividad de los administradores y generación de alertas de incumplimiento de políticas.

Las políticas aquí fijadas hacen parte integral de la Política general de seguridad y privacidad de la información que entró en vigencia a partir del el 01 de julio de 2020, la cual fue revisada y aprobada por el Comité Institucional de Gestión y Desempeño, en asesoría de la mesa técnica de Gobierno y seguridad digital el día 18 de junio de 2020 (Acta 002 de 2020). Este manual se actualiza para dar cumplimiento a los lineamientos de la política general.