LISTA DE VERSIONES:

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	12/05/2014	Se actualizó el alcance, se incorporaron documentos relacionados, se ajustaron las responsabilidades, se establecieron políticas conforme a estándar ISO 27001 para un Sistema de Gestión de Seguridad de la Información.
2	15/Nov/2016	Se realizó ajuste de objetivos, alcance, condiciones generales y documentos relacionados, actualización de definiciones relacionadas con tipos de datos, clases de información, preservación de documentos; se ajustan las responsabilidades en seguridad de la información, se actualizaron las políticas 1, 4, 5 y 11 relacionadas con: clasificación, ordenación y protección de la información y de los datos, copias de seguridad de archivo de datos y retención de copias de seguridad, uso aceptable para correo electrónico y otros servicios de Internet, gestión de incidentes en la seguridad de la 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 la misma, y estableciendo objetivos organizacionales para la protección de sus activos de información, así como las responsabilidades y los derechos que deben conocer y cumplir los usuarios clientes internos y externos, propietarios 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 apegado 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

La política de seguridad de la Información es 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 (funcionarios, 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 la infraestructura tecnológica de la entidad.

Todos los usuarios contarán 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 acción disciplinaria.

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 Estrategia de Gobierno en Línea para la implementación del Modelo de Seguridad de la Información.

En este documento no se establecen políticas de continuidad y recuperación de desastres, para ello se cuenta con otros documentos de políticas, estrategias y procedimientos necesarios para aplicación del tema.

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 ó de un remitente cuando hace una petición de comunicación controlandose el acceso hacia algún recurso. El usuario ó 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 ó 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 ó distribuyen como mensajes ó archivos.

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 ó 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 ó un servicio de TI.
Usuario administrador de sistemas: Es un profesional universitario ó 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, y ley 1712 de 2014.

4. DOCUMENTOS RELACIONADOS

Modelo de seguridad de la información para la estrategia de Gobierno en Línea
Manual para la implementación de la Estrategia de Gobierno en Línea de la Republica de Colombia
Plan de desarrollo “Creemos en Boyacá, tierra de paz y libertad 2016-2019”

5. CONDICIONES GENERALES

Normatividad:

Ley 527 de 1999
Ley 1273 de 2009
Ley 1266 de 2008
Ley 1581 de 2012

Ley 1712 de 2014
Decreto 1377 de 2013
Decreto 2609 de 2012
Decreto 415 de 2016
ISO/IEC 27001: 2005
ISO/IEC 27001: 2013

Metas de la Política de Seguridad

En el plan de desarrollo "Creemos en Boyacá, tierra de paz y libertad 2016-2019" se estableció un subprograma de Gestión de Seguridad de la información que tiene por objetivo aumentar el nivel de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y del Sistema de Gestión de Continuidad del negocio que permita garantizar la protección de la información y la continuación de operaciones, así mismo aumentar la capacidad del personal adscrito al proceso Gestión NTICs en temas de seguridad y privacidad de la información. Para ello se establecieron las metas:

- El 65% del Sistema de Gestión de Seguridad de la Información implementado
- El 60% de políticas de continuidad del negocio implementadas
- Un pacto por el teletrabajo firmado con el MinTIC
- 5 Capacitaciones en Seguridad y Privacidad de la Información al personal del proceso de Gestión NTICs realizadas

Adicionalmente se tiene como meta concientizar a los usuarios de la necesidad del buen uso de la las Tecnologías de la Información y Comunicación de la Gobernación de Boyacá, presentando y dando a conocer las responsabilidades y las medidas que se deben adoptar para proteger la infraestructura tecnológica 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 Estrategia de Gobierno en línea.

La gestión de Tecnología de Información y Comunicación de la Gobernación de Boyacá propone esfuerzos de seguridad de la información a través de la Dirección de Sistemas con el proceso de Gestión de NTICs (Nuevas Tecnologías de la Información y la Comunicación) para la implementación de la política de seguridad de la información y de uso de la Infraestructura de Tecnología de Información y Comunicación.

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

De acuerdo a la reciente normativa que plantea el Gobierno nacional bajo el Decreto 415 de 2016 se establece un marco para la Gestión de Tecnologías de Información y tareas de institucionalidad de TI para 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 que junto con el Secretario General son responsables de aprobar las políticas de seguridad de la Información en la Gobernación de Boyacá propuestas por el comité de evaluación de políticas de seguridad o comité de Gobierno en Línea donde el mismo GCIO lidera.

El comité de evaluación de políticas de seguridad o comité de Gobierno en Línea 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 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 a través de un plan de seguridad de la información diseñará y ejecutará la forma de aplicar cada una de las políticas de seguridad.

La Dirección de Control Interno 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, como de los entes judiciales 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 dirección de Control Interno Disciplinario, actuando conjuntamente con la Dirección de Talento Humano.

Las políticas que figuran en este documento también han sido aprobadas, apoyadas y defendidas 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 al comité de evaluación de la política o comité de Gobierno en Línea por medio de los canales electrónicos dispuestos para este propósito (correo electrónico direccion.sistemas@boyaca.gov.co, enlace al buzón de sugerencias o al sistema de mesa de ayuda publicados en la Intranet), quien 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 direccion.sistemas@boyaca.gov.co, enlace al buzón de sugerencias o al sistema de mesa de ayuda publicados en la Intranet) y esta será revisada por el comité de evaluación de la política o comité de Gobierno en Línea quien se encargará de la investigación y aprobación de excepciones.

6. FUNCIONES Y RESPONSABILIDADES

A fin de coordinar los esfuerzos de seguridad de la información, la Gobernación de Boyacá ha dividido las responsabilidades de sus miembros en las siguientes categorías de responsabilidad:.

- **Responsabilidades del Propietario**

Los propietarios de los activos de información son en general los Secretarios, Directores o funcionarios asignados por la Gobernación de Boyacá, quienes adquirieren y mantienen las aplicaciones operativas que apoyan la toma de decisiones y otras actividades de la organización.
Cada aplicación de software debe tener un propietario designado.
Los propietarios deben indicar la clasificación que mejor refleja el carácter sensible, el valor crítico y la disponibilidad de cada tipo de información. La clasificación, a su vez, determinará el nivel de acceso de los usuarios.

- **Responsabilidades del Usuario**

Todo el personal que maneja activos de información e infraestructura tecnológica tiene la denominación de usuario y tiene las siguientes responsabilidades:

- Almacenamiento de información de la Entidad, de custodiar la información confiada, de usar el sistema de control de acceso lógico y ejecutar periódicamente copias de seguridad.
- Aplicación, mantenimiento y revisión las medidas de seguridad definidas por los dueños de la información.
- Aplicación las políticas de seguridad de la información, normas, procedimientos y legislación aplicable. Deben comprender perfectamente estos requisitos y cumplir con ellos
- Actualización de la información de registro de inventario de activos
- Identificación del nivel de clasificación de los activos de información
- Aplicación de los controles apropiados para asegurar la confidencialidad, integridad y disponibilidad de la información
- Aplicación de medidas de seguridad para garantizar su cumplimiento y reporte de situaciones de incumplimiento

- **Responsabilidades de los Administradores de Información y de recursos TI**

El personal de la Dirección de Sistemas y en general del proceso de Gestión de NTICs son administradores de sistemas y tienen responsabilidad sobre la administración de la información.
Los administradores de información son los servidores públicos que están encargados de la custodia de la información de la Entidad que generalmente se encuentra centralizada en equipos servidores.
Los Administradores de Información son responsables de usar el sistema de control de acceso, y de ejecutar plan de continuidad y contingencia de TI, lo que incluye: copias de seguridad de las bases de datos alojadas en equipos servidores.
Los Administradores del proceso de Gestión de NTICs están facultados para depurar datos e información electrónica según tipo y clasificación conforme a lo establecido en la política de clasificación y ordenación definida en este manual.
El personal de la Dirección de Sistemas está facultado para tomar instantáneas del sistema, reconfigurar, reiniciar, apagar y restaurar cada equipo de cómputo de la Entidad con fines de eficacia en la recuperación del sistema para retornarlo a un estado funcional, y de eficiencia energética.

7. POLÍTICAS DE OPERACIÓN

POLÍTICA 1: CLASIFICACIÓN, ORDENACIÓN Y PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS

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 propietarios manejen, toda la información debe integrarse en una de las

siguientes clasificaciones:

- **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 protección de la información y de los datos

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.

Los usuarios que manipulen datos de carácter personal del ciudadano están obligados a atender las implicaciones de las leyes 1266 de 2008, 1581 de 2012 y sus reformas, por la cual 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 y la proveniente de terceros países, 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. 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 almacenada en un servidor de base de datos deberá estar sometida a mecanismos de protección para garantizar que no sea inapropiadamente descubierta, modificada, borrada y que pueda ser recuperable.

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 propietarios 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.

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), conforme se establece en el Decreto 2609 de 2012.

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 de accesibilidad que define el Director Administrativo de Sistemas de la Gobernación de Boyacá.

Los usuarios externos de la Gobernación de Boyacá, que requieran ingresar a los sistemas de información de la entidad, deberán contar con el visto bueno del Director del área de interés así como la autorización del Director Administrativo de Sistemas.

Los funcionarios públicos deberán firmar un acuerdo o una cláusula contractual de buen uso de la Infraestructura de Tecnología de Información y Comunicación, que incluye la confidencialidad y no divulgación de la información sensible y de la información de carácter personal del ciudadano en procura de la protección y buen manejo de este activo.

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 periodo establecido en las normatividad aprobada de retención documental por la Gobernación de Boyacá.

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 la desactivación de cuentas de acceso (especificando los sistemas en los que se tenía uso) a la Dirección de Sistemas 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 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.

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.

Las identificaciones de usuario deben individualizar a usuarios específicos y ser utilizada con el fin de permitir el acceso al sistema 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.

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 y de los Sistemas de información controlados y almacenados en dichos equipos.

Antes que un nuevo sistema de información se desarrolle o se adquiera por parte de la Gobernación de Boyacá, la Dirección de Sistemas deberá definir 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 de sistemas hasta la conversión a un sistema en producción.

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, y 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; y como mínimo debe tener una longitud de ocho (8) caracteres; la contraseña debe 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.

POLÍTICA 3: 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 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 y las impresoras de la entidad se deberán apagar o poner en estado de suspensión cuando no estén en uso; además, limpiar las impresoras de documentos. Cuando el usuario se retira de su puesto de trabajo, bloquear el equipo (instrucción: ⊞ + L). Los equipos de escritorio estarán obligados a utilizar protector de pantalla protegido con contraseña para que el bloqueo sea automático después de unos minutos de inactividad (entre tres y cinco minutos es razonable).

POLÍTICA 4: COPIAS DE SEGURIDAD DE ARCHIVO DE DATOS Y RETENCIÓN DE COPIAS DE SEGURIDAD

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 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, y la clasificación de la información identificada en instrumentos de recolección de información señalados en la ley 1712 de 2014, la cual será almacenada en discos o medios de propiedad de la Entidad. Cada sectorial o área dueña de la información es responsable de definir e informar a la Dirección de Sistemas cuál es la información que se encuentra y se protege en computadores de escritorio (clientes gruesos) y que no se encuentra en equipos Servidores, para proceder al seguimiento de la realización de copias de seguridad periódicas atendiendo a lo establecido en el Plan 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; los backups se realizarán de acuerdo a las políticas de continuidad y recuperación, al plan de Continuidad del Negocio y Recuperación de Desastres definido por la Dirección de Sistemas y al instructivo de Administración de Recursos de almacenamiento de información.

Se establecerá el procedimiento de copia de seguridad y de recuperación de la información debidamente documentado, se definirá la extensión, frecuencia y periodo de retención de las copias de seguridad de conformidad con los requisitos de seguridad de la información y la importancia de la información para el funcionamiento continuo de la entidad.

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

Se establecerá 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.

Adicionalmente y por seguridad de la información, deberá establecerse procedimiento para la gestión de los soportes extraíbles, que aseguren la protección de la información.

POLÍTICA 5: USO ACEPTABLE PARA CORREO ELECTRÓNICO Y OTROS SERVICIOS DE INTERNET

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 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."
- No se deben enviar mensajes no solicitados que son excesivos y/o destinados a acosar o molestar a los demás (spam) ya que afecta gravemente la eficiencia y costo-beneficio del servicio.
- 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.
- Las comunicaciones oficiales por parte de los funcionarios públicos deben ser enviadas y recibidas a través de la dirección de correo electrónico institucional proporcionada por la Dirección de Sistemas. Las cuentas personales de correo electrónico no pueden ser usadas para tal fin.
- 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, dirección y número de teléfono.
- Los servicios de correo electrónico solo podrán utilizarse con fines lícitos; no se debe constituir marketing engañoso, no se debe mantener contenido obsceno, ofensivo, difamatorio, abusivo, o fraudulento.
- 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.
- No violar las normas del proveedor del servicio de correo electrónico
- 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 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 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.
- 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.
- El servicio de correo electrónico institucional puede ser retirado a un usuario o su cuenta desactivada en cualquier

momento, a discreción de la Administración, si se observa un uso indebido o un alto porcentaje de recepción de mensajes spam.

- Los Directivos solicitarán la creación, reinicio o cancelación de las cuentas electrónicas para personal de planta según funciones asignadas y será validada con la información reportada por la Dirección de Gestión de Talento Humano.
- 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.
- 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. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe reenviar el correo sospechoso a la cuenta soporteweb@boyaca.gov.co con la frase “correo sospechoso” en el asunto.
- Las cuentas de correo electrónico 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 y no debe utilizarse para otro fin.
- Periódicamente el administrador de cuentas revisará las cuentas que llevan más de 60 días sin ningún acceso. En caso tal, se procederá a enviar una comunicación de dichas cuentas sin uso advirtiendo del proceso de desactivación 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 la solicitud de no desactivación, se procederá a la desactivación y se entenderá que el usuario ya ha sido comunicado.
- 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 desactivada.
- Las cuentas de correos que permanezcan con estado desactivado se conservarán por el término de un (1) año, después de ese lapso de tiempo se realizará el proceso de eliminación.
- Los correos electrónicos deben contener la siguiente nota respecto al manejo del contenido:
  “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 soporteweb@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.

POLÍTICA 6: ADMINISTRACIÓN DE CAMBIOS

Para la administración de cambios de las Tecnologías de Información y Comunicación se efectuará el procedimiento correspondiente definido por la Dirección de Sistemas de la Gobernación de Boyacá, de acuerdo con el tipo de cambio solicitado y la infraestructura tecnológica relacionada.

Todo cambio (creación y modificación de programas, pantallas y reportes) que se necesite a las aplicaciones informáticas, debe ser requerido por los usuarios de la información mediante el formato "requerimientos para investigación y desarrollo" y deberá ser aprobado formalmente por la Dirección de sistemas. Los responsables de la administración de las aplicaciones tendrán la facultad de aceptar o rechazar la solicitud, bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por el usuario, o un tercero externo.

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 por la Dirección de Sistemas.

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; y se registrará el cambio de repuesto o reparación en la hoja de vida del equipo.

Los equipos de cómputo: Desktop (cliente grueso), Servidores, Thin Client (clientes liviano), Workstations; las impresoras no deben moverse o reubicarse sin la aprobación previa del Director de Sistemas, jefe o coordinador del área involucrada.

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.

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.

POLÍTICA 7: 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.

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.

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. Un filtrado web ayudará a proteger contra las amenazas basadas en Web impidiendo que los usuarios accedan a sitios de phishing conocidos 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.

El servicio de acceso a la Intranet por el portal de la Gobernación en Internet se prestará con restricciones de acuerdo a políticas de Firewall definidas para proporcionar una conectividad confiable y controlar ataques informáticos por la red.

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

POLÍTICA 8: SEGURIDAD PARA USUARIOS TERCEROS

Una vez contratados servicios de TI por outsourcing deberán negociarse y aclararse, dentro del contrato, las políticas y procedimientos para asegurar que los objetivos de seguridad del Sistema se sigan cumpliendo: efectividad, eficiencia, adecuación, integridad, validez, autorización y privacidad.

Los recursos informáticos que no sean propiedad de la Entidad y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento.

Cuando se requiera utilizar las Tecnologías de Información y Comunicación de la Gobernación de Boyacá para el funcionamiento o el alojamiento de elementos tecnológicos que no sean propios de la entidad y que deban ubicarse en sus instalaciones serán administrados por la Dirección de Sistemas de la Gobernación de Boyacá.

Los usuarios contratistas o terceros, tendrán acceso a los Recursos Informáticos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien sea su Jefe inmediato, Interventor o Supervisor.

Los contratistas deberán firmar y renovar dentro de cada contrato, un acuerdo de buen uso de los Recursos Informáticos, confidencialidad y no divulgación de la información sensible y de la información de carácter personal del ciudadano; en cumplimiento de la seguridad y buen manejo de la información. Después de que el trabajador deja de prestar sus servicios a la Entidad, está obligado a entregar toda la información respectiva del trabajo realizado se debe comprometer a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la Entidad.

La conexión entre sistemas de información internos y otros de terceros, debe ser aprobada y certificada por la Dirección de Sistemas 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.

Como requisito para interconectar las redes de la entidad con las de terceros, los sistemas de comunicación de terceros deben cumplir con las políticas de seguridad establecidas por la Gobernación de Boyacá. La Gobernación de Boyacá 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 Dirección de Sistemas y la dependencia interesada.

Los proveedores y/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 las funciones a su cargo.

POLÍTICA 9: PROPIEDAD INTELECTUAL Y ADMINISTRACIÓN DE LICENCIAS DE SOFTWARE

La propiedad intelectual desarrollada o concebida mientras el trabajador 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 memos, planes, estrategias, productos, programas de aplicación, documentación y otros materiales.

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 están autorizados para realizar cambios en el software de los equipos oficiales, se sugiere que para se tenga en cuenta la información establecida oficialmente en la cartilla práctica sobre piratería del Convenio Antipiratería para Colombia (http://www.convenioantipirateria.org).

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.

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 deberán desinstalarse una vez caduque la licencia.

La instalación de software debe ser autorizada y realizada por funcionarios de la Dirección de sistemas. 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 10: CONTROL DE ACCESO FÍSICO

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

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

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.

Todos los computadores portátiles, módems y equipos de comunicación sean de la entidad, de terceros o de otros usuarios de la Gobernación de Boyacá deberán ser registrados a su ingreso y salida del edificio en un libro o sistema de registro; para el caso de equipos de la Entidad no podrán abandonar las instalaciones a menos que estén acompañados por la autorización respectiva y la validación de la Dirección de Sistemas.

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

Los computadores portátiles deberán estar protegidos por cables de seguridad, u otros dispositivos de protección contra el robo cuando estén situados en un entorno no controlado, en horas no laborables deberán almacenarse en lugares cerrados con llave.

POLÍTICA 11: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Los usuarios deberán comunicar incidencias de manera oportuna a través de los diferentes canales dispuestos para tal fin a la Dirección de Sistemas para que sea atendido por un Administrador del sistema; los incidentes que no puedan resolverse de forma inmediata serán escalados apropiadamente de acuerdo a los procedimientos adecuados con el propósito de tomar acciones efectivas para minimizar el impacto.

Para gestionar los incidentes de Seguridad de la Información deberá existir un grupo con conocimientos en el manejo de incidentes en las Áreas de Seguridad de la Información.

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

Se debe llevar un registro detallado de los incidentes de Seguridad de la Información y 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 Dirección de Sistemas deberá propender por la adquisición de herramientas que faciliten el proceso de gestión de incidentes de Seguridad de la Información.

Los siguientes son incidentes de exposición de seguridad, que deberán tener registro en documento electrónico o físico:

- Persistencia de infección por virus, u otro código malicioso en cualquier computador después de que el antivirus ha escaneado discos
- Virus, gusanos, troyanos o cualquier otro malware con un impacto significativo sobre la confidencialidad, la disponibilidad y la integridad de una aplicación crítica, de un servicio o de la red
- Instalación de software ilegal o no licenciado en los equipos de cómputo de la Entidad
- Intentos de acceso no autorizado o intrusión en los sistemas de información, ya sea exitoso o no
- Escaneo o sondeo de la red por cualquier usuario no autorizado
- Acceso con perfil de administrador desde alguna cuenta de usuario legítima, realizado por usuario no autorizado
- Pérdida o robo de un activo de Tecnología de la Información
- Fraude, daño, o pérdida de información sensible o de uso interno
- Revelación no autorizada de información sensible, de contraseñas, o de información de uso interno
- Pérdida de computadores de la Gobernación de Boyacá o de computadores personales no institucionales que contengan información sensible o de uso interno sin encriptar.
- Vulnerabilidades encontradas en la red de información
- Violación de las políticas de seguridad de la información

Una vez verificada por la Dirección de sistemas 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 reportará a Control Interno Disciplinario para que se coordine y determine el alcance a las investigaciones según sea el caso.

POLÍTICA 12: 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.

La Dirección de Sistemas divulgará, las políticas, estándares y procedimientos en materia de seguridad informática. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará a la dirección General los casos de incumplimiento con copia a las oficinas de control interno.

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.

Registros de auditoría

Todos los sistemas automáticos 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, 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.

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 del Director de Sistemas.

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.
- 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 Dirección de Control Interno Disciplinario.
- La Administración se reserva el derecho de confiscar cualquier material ofensivo o información ilícita.
- La política aquí fijada entra en vigencia a partir del 09 de mayo de 2014, es comunicada y entendida en todos los niveles de la Entidad a los que afecta y cuenta con el total compromiso y apoyo de la Secretaría General de la Gobernación de Boyacá, quién la establece, aplica y revisa a través de la Dirección de Sistemas.

ELABORO		REVISO		APROBO	
Nombre:	Facilitador SIG - MÓNICA ORDUZ VALBUENA	**Nombre:**	SECRETARIO GENERAL	**Nombre:**	Representante de la Alta Dirección
Cargo:	PROFESIONAL UNIVERSITARIO 219	**Cargo:**	SECRETARIO DE DESPACHO 020	**Cargo:**	REPRESENTANTE DE LA ALTA DIRECCIÓN
Fecha:	15/Nov/2016	**Fecha:**	15/Nov/2016	**Fecha:**	16/Nov/2016