Fecha del plan:	20 / 01 / 2020	**Año de vigencia del plan:**	2020

CONTROL DE CAMBIOS

Versión[1]	Fecha	Cambios introducidos
2015	15/05/2015	Emisión
2017	25/07/2017	Adaptación requisitos ISO 27001:2013 y programas estratégicos
2018	30/07/2018	Se incluye introducción, referencia al plan de tratamiento del riesgo, interesados clave, gestión del cambio, acciones de mejora.
2019	22/01/2019	Se actualizan las responsabilidades, procedimientos, acciones de mejora e indicadores de seguimiento.
2020	20/01/2020	Se actualiza para incorporar procedimiento Gestión de activos de Tecnologías de la información, aspectos de Seguridad digital basada en gestión de riesgos según documento CONPES 3854 de 2016 y en el MGRSD, así como el cronograma de plan de trabajo en cuatro fases.

Elaboró:

Versión	Nombre Autor (es)	Cargo o Profesión
2015	Mónica Orduz Valbuena	Profesional Universitario
2017	Mónica Orduz Valbuena	Profesional Universitario
2018	César Augusto Sánchez Aguilar	Profesional Externo
2019	Fabián Ricardo Corredor	Profesional Externo
2020	Mónica Orduz Valbuena Fabián Ricardo Corredor	Profesional Universitario Profesional Externo

Revisó:

Versión	Responsable	Cargo o Profesión
2015	Fredy Alexander Siachoque Herrera	Director de Sistemas
2017	Will Yhonatan Amaya Medina	Director de Sistemas
2018	Will Yhonatan Amaya Medina	Director de Sistemas
2019	Will Yhonatan Amaya Medina	Director de Sistemas
2020	Will Yhonatan Amaya Medina Mesa técnica de Gobierno y Seguridad Digital	Director de Sistemas Profesionales de Mesa técnica de Gobierno y Seguridad Digital

[1] Es el año de última actualización dentro del horizonte estratégico o período de gobierno.

Aprobó:

Versión	Responsable	Cargo o Profesión
2015	José Raimundo Pabón Jiménez	Secretario General
2017	Ana Carolina Espitia Jeréz	Secretaria General
2018	Comité de Gobierno en Línea	Miembros del Comité
2019	Comité Institucional de Gestión y Desempeño	Miembros del Comité y profesionales de Mesa técnica de Gobierno y Seguridad Digital
2020	John Amaya Rodríguez Comité Institucional de Gestión y Desempeño	Secretario de TIC y Gobierno Abierto Comité Institucional de Gestión y Desempeño

Colaboradores: Funcionarios y contratistas de la Dirección de Sistemas.

DERECHOS DE AUTOR

1. OBJETIVOS

- Planear, organizar, dirigir y controlar actividades que permitan la integridad, disponibilidad y confidencialidad de los activos de información y comunicación, así como resguardar los activos de Tecnologías de Información de la Gobernación de Boyacá, aplicando las mejores prácticas y estándar de seguridad de la información.
- Establecer los lineamientos y las responsabilidades de los actores que intervienen en la política de seguridad digital de la entidad para que conozcan sobre su implementación desde una perspectiva basada en riesgos de seguridad digital.
- Capacitar, concientizar y empoderar a los usuarios de activos de información (digitales, físicos) sobre la seguridad de la información de la Gobernación de Boyacá.

2. ALCANCE:

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, siendo partes interesadas para la Seguridad digital del territorio.

Este documento establece un plan de seguridad y privacidad de la información que define lineamientos para la aplicación de las políticas de seguridad definidas en el manual de políticas de seguridad de la Información el cual tiene un ámbito de aplicación a todas las sectoriales en primera línea de defensa de los activos de tecnologías de la información; es decir deben involucrarse Secretarios, directivos, funcionarios públicos, contratistas, proveedores y demás usuarios internos y externos de las tecnologías de información de la entidad.

Este documento da aplicabilidad a las cinco fases del Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el MinTIC: Diagnóstico, Planificación, implementación, evaluación de desempeño, mejora continua.

3. DOCUMENTOS RELACIONADOS / LISTA DE REQUISITOS LEGALES Y NORMATIVOS

- Política nacional de Seguridad digital, documento CONPES 3854 de 2016
- Manual de Políticas de Seguridad de la Información, Cód. interno No. A-AD-TI-M-001
- Procedimiento de Gestión de Seguridad de la Información, Cód. interno No. A-AD-TI-P-002
- Procedimiento de Gestión de Activos de Tecnologías de la Información, Cód interno No. A-AD-TI-P-008

- Procedimiento de Administración de riesgos, Cód. interno No. E-DO-DM-P-002
- Procedimiento de Seguimiento de riesgos, Cód. interno No V-EG-P-002
- Instructivo Gestión de Incidencias y Solicitudes de Servicio de TI, Cód. interno No. A-AD-TI-I-001
- Instructivo Administración de cuentas de usuario y perfiles de acceso, Cód. Interno No. A-AD-TI-I-014
- Instructivo Administración y actualización de los servicios de antivirus, Cód. Interno No. A-AD-TI-I-011
- Requisitos definidos en estándar ISO/IEC 27001
- Términos y definiciones en estándar ISO/IEC 27000
- Marco de interoperabilidad y modelo de seguridad señalados por el Gobierno Nacional a través del Decreto 2693 de 2012
- Lineamientos generales de la política de Gobierno Digital, según decreto 1008 de 2018, MinTIC
- Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas, MinTIC
- Directrices para la integración de planes institucionales y estratégicos al plan de acción por parte de las entidades del estado según decreto 612 de 2018
- Manual de Gobierno digital, MinTIC
- Modelo de Seguridad y Privacidad de la Información (MSPI), MinTIC
- Modelo nacional de Gestión de Riesgos de Seguridad Digital (MGRSD), MinTIC
- Guía de Administración del Riesgo y diseño de controles en entidades públicas, DAFP

4. DEFINICIONES

Para el propósito de este documento se aplican términos y definiciones dados en ISO/IEC 27000, y además los descritos en glosario del Modelo nacional de Gestión de Riesgos de Seguridad Digital (MGRSD).

5. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

5.1. Competencias, funciones y responsabilidades

Los funcionarios deben tener conocimientos básicos de las Tecnologías de Información y del Sistema de Gestión Documental, como lo indica el Manual de funciones y competencias laborales de la Entidad. Es obligación de los funcionarios que tengan a cargo o sean responsables de archivos públicos velar por la integridad, autenticidad, veracidad y fidelidad de la información de los documentos de archivo, sean estos físicos o electrónicos, y serán

responsables de su organización y conservación, de acuerdo a lo dispuesto en la Ley general de archivos.

Los profesionales encargados de la Gestión de Seguridad de la Información deben conocer y tener experiencia sobre: gestión del riesgo de TI, implementación de políticas de seguridad y privacidad de la información; así como, mecanismos y herramientas de control para la protección de activos de información, la operación de todos los componentes y servicios del SGSI.

El Secretario de TIC y Gobierno abierto será el responsable de liderar la implementación de la Política de Gobierno Digital, y el Director de sistemas de información de liderar la implementación de la política de seguridad digital, según decreto Departamental 318 de 29 de mayo de 2019.

El Secretario de TIC y Gobierno abierto y demás integrantes de la mesa técnica tienen el objetivo de "Orientar y coordinar la implementación, seguimiento y evaluación de la política de Gobierno y Seguridad Digital, en la Gobernación de Boyacá" según decreto departamental 318 de 2019, son los responsables de proponer mecanismos, metodologías, lineamientos y procesos específicos para dar cumplimiento a las normatividad relacionada con seguridad y privacidad de la información; coordinar la formulación y actualización de la política general de seguridad y privacidad de la información, el plan y el manual correspondiente para preservar la seguridad y privacidad de la información de la entidad, garantizando el buen uso, confidencialidad, integridad y disponibilidad de esta; coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y transparente; proponer y hacer seguimiento al plan de seguridad y privacidad de la información. Adicionalmente, son responsables de realizar la declaración de aplicabilidad de los requisitos normativos, las mejoras a las políticas y al plan de seguridad digital, conforme la norma ISO/IEC 27001.

La Oficina de Control Interno de Gestión tiene la responsabilidad de hacer seguimiento en el cumplimiento de las políticas y plan de seguridad y privacidad de la información; así mismo, de hacer seguimiento a la gestión de riesgos.

La acción disciplinaria en respuesta a las violaciones de las políticas de seguridad de información es responsabilidad de la oficina asesora de Control Interno Disciplinario, actuando conjuntamente con la Dirección general de Talento Humano.

El responsable del proceso de Gestión de Tecnologías de la Información y la alta Dirección son los encargados de enviar a aprobación del comité institucional de gestión y desempeño el plan de seguridad y privacidad de la información y el documento de declaración de aplicabilidad de la norma ISO/IEC 27001.

5.2. CATEGORIAS DE RESPONSABILIDAD

Teniendo en cuenta la importancia que la entidad defina las necesidades de sus grupos de interés para la definición y aplicación de políticas y planes, en la **tabla 1** se encuentra el análisis de interesados clave en seguridad para establecer una política para su uso y apropiación, además, que tenga en cuenta el marco general del funcionamiento de la entidad con propósitos de empoderamiento de los diferentes grupos de valor.

Tabla 1. Análisis de interesados clave de Gobernación de Boyacá

TIPO	LISTA DE GRUPOS DE INTERES		INTERNO / EXTERNO	INFLUENCIA					
	Tipo de vinculación	Rol y/o cargo		Objetivo	Alcance	beneficio obtenido	Toma de decisiones	Grado de influencia	Tipo de influencia
Directivo	Funcionario	Directivo	Interno	Alto	Alto	Alto	Alto	Alto	Positiva
Profesional	Funcionario	Profesional	Interno	Alto	Medio	Alto	Medio	Medio	Positiva
Contratistas	Prestación de servicios profesionales	Contratistas	Interno / externo	Alto	Medio	Alto	Bajo	Bajo	Positiva
Ciudadanos y/o entidades	N/A	Ciudadanos y/o entidades	Externo	Alto	Medio	Alto	Bajo	Medio	Positiva

A fin de coordinar los esfuerzos de seguridad de la información, a continuación se establecen responsabilidades en tres categorías:

Responsabilidades del Propietario:

Los propietarios de los activos de información designados en primera línea de defensa son en general los Secretarios, Directores o funcionarios designados por la Alta Dirección, quienes adquirieren y mantienen las aplicaciones operativas y auto controlan los procesos.

La información agrupada por cualidades y funciones es identificada, clasificada y tipificada. Cada propietario debe indicar la clasificación que mejor refleja el carácter sensible, el valor crítico y la disponibilidad de cada tipo de información y de cada activo de tecnologías de información, teniendo en cuenta políticas de seguridad y privacidad de la información y procedimientos establecidos.

La gestión de riesgos de seguridad digital será liderada por el propietario de los activos de TI y quien establecerá las medidas de seguridad para minimizar el impacto de los mismos.

Responsabilidades del Usuario:

Los usuarios son responsables de almacenar información de la Entidad, de custodiar la información y los activos de TI confiados, de proteger los datos de carácter personal relativo a ciudadanos y solicitantes de trámites y servicios, de usar el sistema de control de acceso lógico y ejecutar periódicamente copias de seguridad. Los usuarios también están obligados a aplicar, mantener y revisar las medidas de seguridad definidas por los dueños de la información.

Los usuarios deberán seguir las políticas de seguridad de la información, normas, procedimientos y legislación aplicable a seguridad digital. Deben comprender perfectamente estos requisitos y cumplir con ellos.

Responsabilidades de los Administradores de TI:

El Director y el responsable del proceso de Gestión de Tecnologías de la Información, en segunda línea de defensa, y los profesionales de la Dirección de Sistemas de información son administradores de sistemas y tienen responsabilidad sobre la administración y protección de la información centralizada en Centros de Procesamiento datos. También, son responsables los funcionarios que se deleguen para coordinar procesos o proyectos donde se capture, procese y se distribuya dicha información.

El Director de Sistemas de Información líder de la implementación de la política de seguridad y privacidad de la información de la entidad es el responsable de consolidar la información de activos de TI y de gestión de riesgos digitales de todas las sectoriales y establecer el plan de tratamiento de riesgos de seguridad y privacidad de la información.

Los administradores de información están facultados para depurar, de los equipos servidores y estaciones de trabajo, archivos electrónicos tipo multimedia que sean de carácter personal de los funcionarios una vez sean identificados y se determine la relevancia para los propósitos de la Entidad, haciendo transferencia a medios propios de los usuarios y liberando capacidad de disco en los equipos.

El personal de la Dirección de Sistemas está facultado para tomar instantáneas del sistema, reconfigurar, hacer copias de seguridad, reiniciar, apagar y restaurar cada equipo de cómputo de la Entidad con fines de control de incidencias de seguridad.

6. GESTIÓN Y TRATAMIENTOS DE RIESGOS

6.1. Plan de tratamiento de riesgos

A partir de la evaluación del diagnóstico de seguridad de la información realizado por la Dirección de sistemas de información, de la gestión de activos de TI y la Gestión de riesgos digitales realizada por las sectoriales, conforme al procedimiento A-AD-TI-P-008, se investigará y analizará los riesgos asociados a la seguridad de la información en los procesos de la Gobernación de Boyacá.

Los riesgos de seguridad de la información y su gestión se consolidan y se podrán consultar en el plan de tratamiento de riesgos de la seguridad de la información.

La administración y seguimiento de los riesgos identificados se hará periódicamente y conforme a los procedimientos No V-EG-P-002 No. E-DO-DM-P-002 de los procesos Direccionamiento y Mejoramiento del Sistema y Evaluación Independiente respectivamente.

6.2. Mapa de riesgos de seguridad y privacidad de la información

En el mapa de riesgos de cada sectorial se registrará la identificación de los riesgos de seguridad digital y el tratamiento de cada uno, en el plan de tratamiento de riesgos de seguridad y privacidad de la información se establecerá los lineamientos y el plan de trabajo para abordar la seguridad y privacidad de la información basada en esos riesgos.

7. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La política de alto nivel o política general de la Gobernación de Boyacá, aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI.

La Política General de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la Gobernación con respecto a la protección de los activos de información, que soportan los procesos de la entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información. Adicionalmente, las políticas establecidas en el Manual de Políticas de Seguridad de la Información, Código Interno No. A-AD-TI-M-001 hacen parte integral de la política general.

De esta forma, una buena política es concisa, fácil de leer y comprender, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción. En el caso, la política general es corta y enmarca los principios que guían las actividades dentro de la entidad.

8. SEGURIDAD POR EL RECURSO HUMANO

Identificadas las condiciones de seguridad de la información declaradas en los documentos de la etapa precontractual y contractual para la vinculación de las personas, o en actas de entrega del cargo, donde los usuarios, propietarios y administradores se comprometen formalmente en la protección de información que se les confía. En caso de ausencia de dicho compromiso formalizado contractualmente, se establece un acuerdo de buen uso, confidencialidad y no divulgación de la información sensitiva y de la información de carácter personal del ciudadano en procura de la protección y buen manejo de este activo.

Con lo anterior, si algún trabajador, funcionario o contratista, deja de prestar sus servicios a la Entidad, o se traslada a otra dependencia asegura el retorno total de la información que gestionó durante el ejercicio de sus funciones, se obliga a no utilizar, comercializar o divulgar los productos o la información generada durante su gestión en la Entidad, por el periodo establecido en la normatividad aprobada de retención documental por la Gobernación de Boyacá.

La Dirección de Sistemas mediante el monitoreo de registros automáticos de eventos en las diversas plataformas tecnológicas 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.

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.

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.

El incumplimiento de la política de seguridad de la Información conllevará medidas de carácter administrativo o disciplinario necesarias para garantizar la normalización de la situación, subsanar el evento sucedido o eliminar la causa raíz que generó la incidencia de seguridad. La Gobernación de Boyacá está en la obligación de imponer las medidas sancionatorias a que haya lugar atendiendo lo contemplado en el artículo 23, 27, 34 de la ley 734 de 2002 por la cual se expide el código disciplinario único en Colombia.

9. GESTIÓN DE ACTIVOS

Para la gestión de activos de TI se implementará el procedimiento A-AD-TI-P-008. El inventario de activos de Tecnologías de Información en lo relacionado a Hardware y Licencias de Software se registrará y se gestionará a través del inventario de activos de infraestructura de TI y la Base de Datos de Gestión de la Configuración (CMDB) implementada en la herramienta de mesa de ayuda para la Gestión de Activos.

Sobre el inventario y la clasificación de activos se determinará el nivel de protección a proveer para cada uno de ellos, identificando el responsable.

Para el inventario de activos de información cada sectorial desarrollará su parte del catálogo de activos de información; en relación a los sistemas y servicios de información, se desarrollará en el catálogo de servicios de información; Los propietarios de la información deberán clasificar la información conforme a la ley de transparencia y acceso a la información, de acuerdo a las siguientes categorías:

- Información pública
- Información pública clasificada
- Información pública reservada

Según la Política 1: Clasificación, ordenación y protección de la información y de los datos del Manual de seguridad y privacidad de la información:

En cuanto a la clasificación y priorización de los sistemas de información se establecerá una matriz de "priorización de sistemas de información frente a sus características", para definir el nivel de protección para cada uno de estos sistemas de información. Se realizará priorización de acuerdo al grado de afectación en posible materialización de riesgos, y analizando criterios, como: impacto, cobertura, necesidad de infraestructura, sistemas vinculados, interoperabilidad, entre otros. La información y sistemas de información tendrán copias de respaldo conforme a lo establecido en el Manual de Políticas de Seguridad de la Información.

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 cuatro subniveles de almacenamiento (subcarpetas), conservando la ordenación de archivos definida en la Tabla de Retención Documental (TRD) que le corresponda. El nombre de un archivo incluirá: la ruta desde el directorio raíz, la carpeta y las subcarpetas, el nombre y extensión del archivo; la ruta no deberá superar los doscientos cincuenta y cinco (255) caracteres.

Los medios que almacenan información electrónica se tendrán que organizar y etiquetar de acuerdo al esquema de clasificación y de conformidad al código de identificación documental; cada administrador o propietario dispone o autoriza remover o transferir información evitando el mal uso.

10. CONTROL DE ACCESO

De conformidad a la Política 2. Control de acceso a la información y a las aplicaciones, del Manual de seguridad y privacidad de la información se establecerán mecanismos de identificación, autenticación y roles / grupos de privilegios de usuario apropiados según la clase de información y el tratamiento que se autorice a la misma.

Es decir, se crearán cuentas de acceso a los sistemas donde se pueda identificar al usuario y se le permita una autenticación mediante contraseña; lo anterior, siguiendo el instructivo Administración de cuentas de usuario y perfiles de acceso de Cód. Interno No. A-AD-TI-I-014.

La identificación de cada usuario o ID en los sistemas se define de manera individual para permitir el acceso controlado con determinado nivel de seguridad de acuerdo a sus funciones, responsabilidades y actividades.

Los niveles de seguridad de acceso que se definen para tener ingreso a la información necesaria y suficiente:

Tabla 2. Nivel de seguridad de acceso de Gobernación de Boyacá

Nivel de seguridad de acceso	Permisos / Privilegios			
	Consulta	Adición	Edición Modificación	Eliminación
Muy Alto (Básico)	X			
Alto	X	X		
Medio	X	X	X	
Bajo	X	X	X	X

Fuente: Elaboración propia

La contraseña o clave, como mecanismo de autenticación que el usuario define para el ingreso a cualquier sistema, 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, a más tardar cada 180 días para el caso de aquellos sistemas que no exijan un cambio periódico obligado.

Los sistemas de información y aplicaciones de software tendrán registro de actividades (log) cada vez que los usuarios accedan, con fines de trazabilidad de las operaciones. Conforme se indica en el instructivo Monitoreo de la operación en sistemas de Información de Cód. Interno No. A-AD-TI-I-007.

Los propietarios de la información que es manejada a través de aplicación web o software de sistema de información indicarán mediante un oficio remisorio y en la mesa de ayuda de sistemas el listado de usuarios que se requieren activar dando la autorización o visto bueno para su ingreso al sistema durante un período de tiempo específico, indicando por cada usuario: nombres y apellidos completos, número de identificación personal, número de la tarjeta profesional, correo electrónico.

Si algún usuario deja de prestar sus servicios a la Entidad, o se traslada a otra dependencia terminan todas las prerrogativas para el uso de los sistemas de información. Lo anterior, tendrá que informarse por el propietario de la información si sucede antes del término autorizado inicialmente.

Los usuarios serán provistos con acceso a la red, a los servicios de red y al equipo de cómputo a los cuales ellos tengan autorización específica para usar.

11. SEGURIDAD FISCAL Y AMBIENTAL

Se dará cumplimiento a la Política 10. Control de acceso físico, del Manual de seguridad y privacidad de la información, de tal forma que los centros de procesamiento de datos y los centros de cableado tendrán restricción de acceso a personal que no pertenezca a la Dirección de Sistemas y que no esté debidamente autorizado. Lo anterior, Implementando controles como puerta / muro de seguridad.

El registro de ingreso y salida de los equipos electrónicos se realizará en un libro de control en la entrada principal de cada una de las sedes de la Gobernación de Boyacá. El registro de ingreso y salida de los equipos electrónicos internos pertenecientes a la Entidad se hará mediante el formato de “control de ingreso y salida de elementos y/o equipo” código interno A-AD-SA-F-024.

Los computadores portátiles estarán protegidos por guayas de seguridad, u otros dispositivos de protección contra el robo cuando estén situados en un entorno no controlado, en horas no laborables deberán entregarse a cada responsable de equipo y almacenarse en lugares cerrados con llave.

Sobre la política de escritorio limpio y pantalla limpia 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).

Los elementos existentes para el control de incendios e inundaciones están bajo la Dirección de Servicios Administrativos y Logísticos, como extintores, sensores y alarmas, los cuáles serán instalados principalmente en áreas críticas, como centros de procesamiento de datos y de cableado; la Dirección de Sistemas establecerá medidas preventivas a través del Plan de continuidad del negocio y recuperación de desastres.

De acuerdo a los monitoreos sísmicos, que ha venido realizando el Consejo Departamental de Gestión del Riesgo, el municipio de Tunja está en zona de riesgo intermedio para temblores; no obstante, se declaran alertas y se establecen medidas preventivas a cargo de este organismo. Así mismo, junto con el IDEAM se identifican amenazas ambientales y determinan alertas y medidas preventivas para riesgos de inundación y deslizamientos de tierra. De lo anterior, la Gobernación de Boyacá deberá estar atenta y tomar acciones pertinentes para evitar pérdidas humanas.

12. SEGURIDAD DE OPERACIONES TI

12.1. Procedimientos operacionales

Los procedimientos operacionales existentes se encuentran cargados y publicados en la herramienta del Sistema Integrado de Gestión, para su consulta y aplicación, estos son:

A-AD-TI-P-002 Gestión de seguridad de la información
A-AD-TI-P-005 Servicio de gestión de operaciones en hardware y software
A-AD-TI-P-006 Servicio de gestión de operación en redes y comunicaciones
A-AD-TI-P-007 Servicio de gestión de operaciones en entornos web
A-AD-TI-P-010 Servicio de gestión de operaciones en sistemas de información
A-AD-TI-P-009 Gestión de incidencias y solicitudes de servicio de tecnologías de información

Los instructivos:

A-AD-TI-I-002 Mantenimiento preventivo.
A-AD-TI-I-003 Mantenimiento correctivo
A-AD-TI-I-004 Diseño y desarrollo de soluciones informáticas
A-AD-TI-I-005 Administración de recursos de almacenamiento de información
A-AD-TI-I-006 Capacitación, asesoría y apoyo para el manejo de software y hardware
A-AD-TI-I-007 Monitoreo de la operación en sistemas de información
A-AD-TI-I-008 Monitoreo de la operación de servidores de red
A-AD-TI-I-009 Administración de canales de internet
A-AD-TI-I-010 Soporte al sistema de comunicación telefónico
A-AD-TI-I-011 Administración y actualización de los servicios de antivirus
A-AD-TI-I-012 Instalación y administración del licenciamiento de software
A-AD-TI-I-013 Administración de sitios web institucionales
A-AD-TI-I-014 Administración de cuentas de usuario y perfiles de acceso
A-AD-TI-I-015 Registro de derechos de autor de sistemas de información

Los manuales son:

A-AD-TI-M-001 Políticas de seguridad y privacidad de la información
A-AD-TI-M-003 Publicación en sitio web institucional y política editorial

Todo cambio a un activo de información se realizará acorde a la Política 6: Administración de cambios del manual de seguridad y privacidad de la información, se registrará desde su solicitud hasta su implantación. El mecanismo o herramienta para efectuar el registro y seguimiento que garantice el cumplimiento de los procedimientos definidos será la mesa de servicios TI, de la Dirección de sistemas.

12.2. Protección contra software malicioso

El software antivirus, instalado en los equipos que hacen parte del inventario de la Gobernación de Boyacá, garantizará una protección en tiempo real contra virus informáticos, gusanos, troyanos, spyware, phishing y otras amenazas de malware que provienen de la red.

Se utilizará una consola de administración para monitorear y actualizar los parámetros de las herramientas antivirus.

Se hará instalación y actualización del software antivirus cliente y de las bases de datos de definición de virus de manera periódica de conformidad al instructivo Administración y actualización de los servicios de antivirus Cód. Interno No. A-AD-TI-I-011.

Para los equipos cliente que no soporten el software antivirus principal adquirido, tendrán la opción de instalación de un software antivirus libre avalado y autorizado por la Dirección de Sistemas.

Para controlar instalaciones de software, en los equipos cliente, estas se harán a través del usuario administrador; así mismo, se hará control de descargas de archivos de la red a través del Firewall / Appliance de seguridad.

12.3. Copias de seguridad (backup)

Se debe realizar copia de seguridad de las aplicaciones, bases de datos y bodegas de archivos alojados en equipos servidores. Estas se deben realizar por profesionales de la Dirección de Sistemas y se deberán almacenar en un sitio alterno fuera del edificio donde se encuentre el centro de procesamiento principal.

Se debe realizar copias de seguridad de la información más relevante de acuerdo a la criticidad e impacto de los sistemas de información, y la clasificación de la información almacenada en equipos de cómputo cliente en cada una de las dependencias, esta debe ser ejecutada por un funcionario de la dependencia, de acuerdo a la periodicidad definida en el listado de clasificación de información.

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. Lo anterior, de acuerdo la documento Administración de recursos de almacenamiento Cód. Interno No. A-AD-TI-I-005.

12.4. Registro y monitoreo

Cuando se presenten eventos que pongan en riesgo la integridad, disponibilidad y confidencialidad de la información se deberán registrar y realizar las acciones tendientes a su solución.

Para el registro de incidentes de seguridad se tendrá en cuenta el reporte del incidente que el funcionario público o particular ponga en conocimiento a la Dirección de Sistemas de información a través de la mesa de servicios. El reporte deberá contener información completa y precisa indicando el lugar, la fecha y detalle de los hechos.

La Dirección de Sistemas analizará cada reporte y de acuerdo a su gravedad se elaborará el concepto técnico, se realizarán las acciones tendientes a su solución, como sea procedente según sea el caso; se comunicará el incidente de seguridad a la Dirección de Servicios Administrativos y Logísticos, quien reportará como noticia criminal a las autoridades competentes y a la aseguradora correspondiente; en conjunto se reportará el incidente a la oficina de Control Interno Disciplinario en caso de ser necesario.

En caso de requerirse, solicitar apoyo externo para investigaciones con equipos especializados para hacer informática o cómputo forense. 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.

Para elementos encontrados que puedan ser materia de prueba o evidencia física, los servidores o particulares quienes reportan el incidente tendrán en consideración los lineamientos básicos para el desarrollo de cadena de custodia definidos en el manual de procedimientos para cadena de custodia de la Fiscalía General de la Nación.

Los registros de incidentes serán preservados de acuerdo a los tiempos de retención definidos en las TRD para los requerimientos registrados en la mesa de ayuda.

12.5. Auditoria interna de sistemas de información

La evaluación del Sistema de Gestión de Seguridad de la Información o de Tecnologías de Información en general se hará según la programación de auditorías internas del proceso Evaluación Independiente. Allí se tendrán en cuenta aspectos definidos en los requisitos aplicables de la Norma ISO/IEC 27001:2013 para la Gobernación de Boyacá, establecidos en la declaración de aplicabilidad.

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.

13. SEGURIDAD DE COMUNICACIONES

Se establecerán acuerdos de servicio y niveles de servicio para el acceso y funcionamiento de las redes de datos con los usuarios internos; así mismo, un mecanismo para la administración de requerimientos de red como lo es la mesa de servicios.

Se establecerán acuerdos de servicio y niveles de servicio dentro de los compromisos contractuales con los proveedores para controlar el cumplimiento de requerimientos de servicio en redes de datos y canales de comunicación.

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.

Se contará con un equipo para la seguridad perimetral que contenga servicios de UTM, firewall, VPN, prevención de intrusiones, control de aplicaciones y filtrado de contenidos web. El cual proveerá control avanzado de aplicaciones y permitirá aplicar políticas individuales o por segmentos que se ejecuten a través de la red, que incluya tecnologías para detección de virus / antimalware, anti spam, gestión de vulnerabilidades, y optimización WAN.

Se definirán políticas de filtrado Web dentro del firewall o Appliance de la Gobernación de Boyacá, dependiendo del usuario o grupos de usuario se establecerán perfiles de seguridad y restricciones. Los servidores de aplicaciones y servicios Web internos tendrán protección de tráfico, en cuanto a amenazas ocultas, con tecnologías como la de cifrado SSL.

Se proporcionarán permisos temporales para el intercambio de información al proveedor quien tiene compromisos contractuales de actualización, configuración o mantenimiento de sistemas de información y/o plataformas tecnológicas. Este requerimiento será realizado por el Supervisor del Proveedor en cumplimiento de la Política 8: Seguridad para usuarios terceros, del Manual de seguridad y privacidad de la informaciónb realizando seguimiento de las tareas adelantadas y registrando las actividades hechas.

Se contará con diferentes mecanismos para la protección de transferencia de mensajes electrónicos, como: control por el appliance de seguridad o firewall, controles en el servidor de correo electrónico, incorporación de excepciones dentro de listas negras por la consola de correo electrónico institucional y filtrado de correo electrónico no deseado desde el cliente de correo del usuario final. El servicio de correo electrónico institucional se pondrá a disposición para ser el canal oficial en la comunicación externa de mensajes electrónicos de la Entidad.

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 lineamientos de la Política 5: Uso aceptable para correo electrónico y otros servicios de internet, del Manual de seguridad y privacidad de la información.

El administrador de red deberá cumplir un acuerdo de buen uso, confidencialidad y no divulgación de la información pública clasificada y publica reservada del ciudadano que transita por la red en procura de la protección y buen manejo de este activo.

Se efectuará un monitoreo permanente de la red de datos, canales de comunicación, canal de interconexión de sedes por fibra óptica y red de telefonía para detectar caídas de red o de canal, se registrarán los sucesos y se generarán informes con propósito de tomar acciones para restablecimiento oportuno.

Para los cambios de instalación y configuración de la red y sus diferentes componentes se deberá seguir un plan de acción que permita sistemáticamente una prestación oportuna de los servicios de red minimizando los riesgos de interrupción de la transferencia de información. Estos procesos deben ser liderados por un profesional de la Dirección de Sistemas de información con conocimiento adecuado y los cambios autorizados por el Director.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SERVICIOS WEB Y DE APLICACIONES

La Gobernación de Boyacá cuenta con mecanismos de protección de los Sistemas de Información que proveen servicio sobre redes públicas. La información involucrada en servicios de aplicación que es transmitida sobre la red pública estará protegida de actividades fraudulentas, divulgación y modificación no autorizada, de alteración, duplicación o replicación de mensajes no autorizada.

La seguridad de la información para las aplicaciones web y portales institucionales se diseñará e implementará dentro del ciclo de vida de desarrollo de los sistemas de información siguiendo la política de administración de cambios, y el instructivo “Diseño y desarrollo de soluciones informáticas” con Cód. Interno No. A-AD-TI-I-004.

En caso de reclamaciones que pudieran interponerse por los usuarios o por terceros en relación con posible incumplimiento de las condiciones de uso de los Servicios Web y Aplicaciones de la Gobernación de Boyacá en relación con los derechos de propiedad intelectual, o derechos fundamentales, o si se tiene sugerencias a la Gobernación para mejorar los contenidos de los medios electrónicos deberán dirigirse a la siguiente dirección de correo electrónico: soporteweb@boyaca.gov.co. Una vez notificado a este correo, dicho contenido será automáticamente excluido o mejorado, según sea el caso, del medio electrónico hasta

que quien haya publicado el contenido en disputa haya resuelto el conflicto con quien envía la reclamación.

De igual forma, la Gobernación tiene a su disposición para atender sus PQRD los siguientes canales de comunicación:

Aplicación Móvil: a través de la cual podrá registrar PQRD.
Página Web: www.boyaca.gov.co en la sección de atención al ciudadano.
Atención telefónica: Sede central 7420150, Secretaría de Salud 7420111 (extensión 4135-4136), Secretaría de Educación 7420200.
Atención personalizada: ventanilla única calle 20 N° 9-90 edificio central, Secretaría de Salud avenida colón N° 22 A - 16 parque Santander, Secretaria de Educación carrera 10N°18-68 en Tunja.
Horario de atención al ciudadano lunes a viernes de 8:00 a.m. -12:00 p.m. y 2:00 p.m.-6:00 p.m.

El servicio de Hosting contratado a cargo de un tercero proveedor tendrá obligaciones o compromisos contractuales para garantizar la seguridad de la información. Así mismo, los encargados de administrar las plataformas implementadas internamente para el mantenimiento del portal institucional y de la Intranet tendrán que garantizar una adecuada implementación de controles en dichas plataformas.

15. GESTIÓN DE INCIDENTES DE SEGURIDAD Y PROVACIDAD DE LA INFORMACIÓN

En el Manual de Políticas de Seguridad de la Información se definió la Política 11: Gestión de incidentes en la seguridad de la información.

Los incidentes de seguridad de la información se identificarán y se reportarán con información completa y precisa indicando el lugar, la fecha y detalle de los hechos. Cómo se indicó en la sección de registro y monitoreo, para el registro de incidentes de seguridad se tendrá en cuenta el reporte del incidente que el funcionario público o particular ponga en conocimiento a la Dirección de Sistemas a través de la mesa de servicios.

A dichos incidentes se les dará tratamiento de acuerdo al instructivo Gestión de incidencias y solicitudes de servicio de tecnologías de información de código interno No. A-AD-TI-P-009.

Para gestionar estos incidentes la Gobernación de Boyacá aplicará estándares internacionales y contará con dispositivos y herramientas de control configuradas de tal manera que permitan detectar amenazas y mitigar riesgos. En algunos casos especializados tercerizando servicios.

A continuación se establecen los procedimientos o equipos para la adecuada gestión de incidentes de seguridad de la información:

Tabla 3. Relación de procedimientos, equipos y/o servicio de Gobernación de Boyacá

NUMERAL	INCIDENTE DE SEGURIDAD	EQUIPO / SERVICIO / PROCEDIMIENTO	REFERENCIA
16.1	Ataques maliciosos externos	Equipo Firewall Protección de acceso remoto Control de intentos de acceso no autorizado o intrusiones en sistemas de información	https://wiki.mikrotik.com/wiki/Main_Page Política 7: Seguridad en Telecomunicaciones y Servicios Asociados del Manual de Políticas de Seguridad de la Información.
16.2	Ataques maliciosos internos	Servicio de Antivirus. Mantener las definiciones de virus y el software antivirus actualizado. Limpieza de virus y otros malware en los equipos de cómputo. Programa de concientización y formación sobre seguridad de la información.	Manual Eset endpoint security 5.0 Instructivo Administración y actualización de los servicios antivirus Documento y material del Programa de sensibilización y formación en seguridad de la información.
16.3	Acceso a la red por personas no autorizadas	Cambio semestral de la clave de los access point para acceso a la red inalámbrica Identificación de accesos no autorizados por el Equipo Firewall. Si una persona logra conectar un PC a un punto de red, le aplica la restricción más alta de navegación a internet y será identificado en el Equipo Firewall	Manual del access point https://wiki.mikrotik.com/wiki/Main_Page
16.4	Acceso físico no autorizado	Acceso restringido a los Centros de Procesamiento Programa de sensibilización y formación en seguridad de la información.	Política 10: Control de acceso físico del Manual de Políticas de Seguridad de la Información. Documento y materiales del Programa de sensibilización y

NUMERAL	INCIDENTE DE SEGURIDAD	EQUIPO / SERVICIO / PROCEDIMIENTO	REFERENCIA
			formación en seguridad de la información.
16.5	Pérdida o robo de equipo de cómputo	Programa de sensibilización y formación en seguridad de la información. Inventario de equipos de cómputo. Registro de portátiles de usuarios terceros.	Documento y materiales del Programa de sensibilización y formación en seguridad de la información. Política 8: Seguridad para usuarios terceros del Manual de Políticas de Seguridad de la Información.
16.6	Administración de red inadecuada	Backup trimestral de los equipos servidores, para el caso de una falla humana o física en equipos activos de red. Monitoreo de canales de internet por el administrador de red Verificación de funcionamiento de los servidores en centros de procesamiento.	https://wiki.mikrotik.com/wiki/Main_Page Instructivos: Administración de canales de internet Monitoreo de la operación de servicios de red
16.7	Cambio de datos no intencionado en un sistema de información	Corrección o restablecimiento de registros y bases de datos del sistema de información Soporte por personal de Dirección de Sistemas a través de la mesa de servicios	Instructivos: Monitoreo de la operación en sistemas de información Gestión de Incidencias y Solicitudes de Servicio de TI
16.8	Copias de seguridad defectuosas	Máquina tape Backup de alta capacidad Redundancia de servidores de aplicaciones y de base de datos Respaldo de las copias de seguridad en centro de	Instructivo: Administración de recursos de almacenamiento de información Manual de usuario Instalación y Administración Backup “Tape Backup”

NUMERAL	INCIDENTE DE SEGURIDAD	EQUIPO / SERVICIO / PROCEDIMIENTO	REFERENCIA
		procesamiento alterno.	
16.9	Extracción de información	Control de acceso a la información y puesto de trabajo libre de medios de almacenamiento y de documentos críticos. Soporte por personal de Dirección de Sistemas a través de la mesa de servicios	Políticas 3: Escritorio limpio y pantalla limpia, 2: Control de acceso a la información y a las aplicaciones, del Manual de Políticas de Seguridad de la Información. Procedimiento: Gestión de Incidencias y Solicitudes de Servicio de TI
16.10	Destrucción de archivos	Para casos de información pública clasificada o reservada que esté contenida en medios de almacenamiento que no sea posible recuperar, se garantizará su destrucción total; soporte por personal de Dirección de Sistemas a través de la mesa de servicios.	Instructivo Gestión de Incidencias y Solicitudes de Servicio de TI
16.11	Falsificación de archivos	Aplicación de las directrices contenidas en estándares internacionales Control de acceso a la información en el puesto de trabajo y control de medios de almacenamiento y de documentos críticos. Identificación y autenticación adecuadas.	Norma NTC – ISO 16175-1 “Información y Documentación. Principios y requisitos funcionales para los registros en entornos electrónicos de oficina. Información general y declaración de principios”. Norma NTC – ISO 15801 Gestión de documentos. Política 3: Escritorio limpio y pantalla limpia del Manual de Políticas de Seguridad de la Información.

NUMERAL	INCIDENTE DE SEGURIDAD	EQUIPO / SERVICIO / PROCEDIMIENTO	REFERENCIA
16.12	Instalación de software no autorizado	Administración instalación de software. Implementación de control de acceso para instalación de software.	Instructivo: Instalación y administración del licenciamiento de software Política 6: Administración de Cambios del Manual de Políticas de Seguridad de la Información.
16.13	Ilegalidad en Licenciamientos	Administración del licenciamiento de software. Adquisición de licencias de software como compromiso obligatorio en la adquisición de equipos de cómputo.	Instructivo: Instalación y administración del licenciamiento de software Política 9: Propiedad Intelectual y Administración de Licencias de Software del Manual de Políticas de Seguridad de la Información.
16.14	Mal uso de sistemas de información	Programa de sensibilización y formación en seguridad de la información. Registro y monitoreo de actividades en sistemas de Información	Documento y materiales del Programa de sensibilización y formación en seguridad de la información. Instructivo: Monitoreo de la operación en sistemas de información
16.15	Mal uso de recursos de red	Programa de sensibilización y formación en seguridad de la información. Registro y monitoreo de operaciones en servicios de red.	Documento y materiales del Programa de sensibilización y formación en seguridad de la información. Instructivo: Monitoreo de la operación de servicios de red de datos
16.16	Pérdidas de conectividad	Registro y monitoreo de operaciones en servicios de red. Registro y monitoreo del desempeño de los canales de acceso a Internet. Registro y monitoreo del sistema de comunicación telefónica.	Instructivos: Monitoreo de la operación de servicios de red Administración de canales de Internet Soporte al sistema de comunicación telefónico

NUMERAL	INCIDENTE DE SEGURIDAD	EQUIPO / SERVICIO / PROCEDIMIENTO	REFERENCIA
16.17	Pérdidas de contraseña	Soporte por personal de la Dirección de Sistemas a través de la mesa de servicios. Control de acceso con autenticación de usuarios en los sistemas.	Procedimiento: Gestión de incidencias y Solicitudes de servicio de TI

Fuente: Elaboración propia

16. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Para el propósito de este documento se aplican políticas establecidas en el documento manual de seguridad y privacidad de la información y el Plan de continuidad del negocio y recuperación de desastres Cód. Interno No. A-AD-TI-F-009.

En el Plan de continuidad del negocio y recuperación de desastres, se establecerán estrategias de continuidad de las operaciones y estrategias de recuperación para los servicios de Tecnologías de Información principales y prioritarios. Para ello se contará con un centro de procesamiento de datos alterno ubicado en un edificio diferente a donde se ubica el centro de procesamiento de datos principal.

17. CUMPLIMIENTO

El Normograma del proceso Gestión de Tecnologías de la Información Cód. Interno No. A-AD-TI-T-006, cuenta con normas relacionadas que definen principios, conceptos, sobre el uso eficiente de las redes y del espectro radioeléctrico, el uso de las redes en teletrabajo, derechos de autor, habeas data; así como, el estándar Internacional ISO/IEC 27001 para el Sistema de Gestión de Seguridad de la Información (SGSI) donde se encuentran los requerimientos de seguridad de la información.

Además, para cumplimiento de las normas de propiedad intelectual y derechos de autor, se atenderá lo establecido en la Política 9: Propiedad intelectual y administración de licencias de software, del Manual de seguridad y privacidad de la información, y en los instructivos “Registro de derechos de autor de Sistemas de Información” Cód. Interno No. A-AD-TI-I-015, e “Instalación y Administración del licenciamiento de software” Cód. Interno No. A-AD-TI-I-012. Todo software que utilice la Gobernación de Boyacá será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos.

Los registros importantes serán protegidos de pérdida, destrucción y falsificación conforme se indica en la norma NTC – ISO 16175-1 “Información y Documentación. Principios y requisitos funcionales para los registros en entornos electrónicos de oficina. Información general y declaración de principios”. Además, los requisitos plasmados en la norma NTC – ISO 15801 “Gestión de documentos. Información almacenada electrónicamente. Recomendaciones para la integridad y la fiabilidad”.

El cumplimiento de políticas y estándares de seguridad se garantizará a través de la aplicación de los procedimientos adecuados.

18. CULTURA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA INFORMACIÓN

Se definirá y desarrollara un Programa de sensibilización y formación en seguridad de la información, para desarrollar una cultura en seguridad de la información dentro de la Gobernación de Boyacá, propicia para los diferentes niveles de responsabilidad en la gestión de la seguridad, utilizando recursos o materiales de capacitación que permitan: comunicar las políticas de seguridad de la información, reflexionar sobre las conductas adecuadas para el uso de sistemas de información y activos de información, alfabetización de los usuarios en el tema. Programa que hará un diagnóstico inicial y evaluación intuitiva e individual de los usuarios de Tecnologías de Información y que permitirá la retroalimentación de esos usuarios.

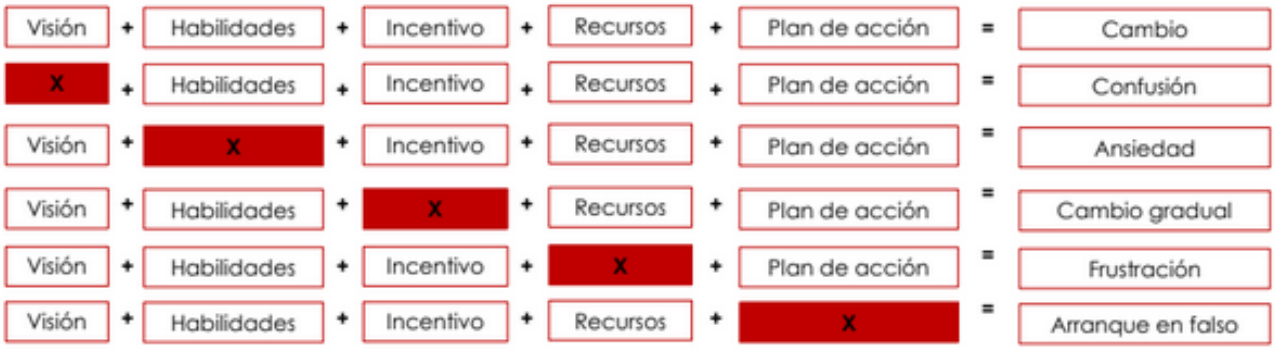
La Dirección de Sistemas y la Dirección de Gestión del Talento Humano trabajaran conjuntamente para el proceso de inducción, capacitación y concientización a los usuarios sobre el uso adecuado de las Tecnologías de Información a su cargo y el cumplimiento de las políticas de seguridad. Se dará a conocer a los usuarios acerca de la acción disciplinaria en la que se puede incurrir en respuesta a las violaciones de las políticas de seguridad de la información.

19. GESTIÓN DEL CAMBIO

Teniendo en cuenta que el cambio es el fenómeno en donde intervienen dos conceptos bien identificados; una situación inicial de la que queremos salir y una situación objetivo que juzgamos como ventajoso y un tercer concepto, más difuso el de la transición. La transición es la situación intermedia donde se nota las dificultades y los costos del cambio y donde no hemos abandonado totalmente las desventajas originales ni hemos obtenido los beneficios que esperamos. http://evolutionchange.com/.

Para el éxito del cambio en una entidad como la Gobernación de Boyacá es importante tener en cuenta los fundamentos presentes en el siguiente modelo de Cambio:

Tabla 4. Fundamentos para el éxito del cambio de Gobernación de Boyacá



Fuente: http://evolutionchange.com/

De acuerdo con el desarrollo de modernización y renovación tecnológica, el proceso de Gestión de TI viene incorporando y adaptando las mejores prácticas para la gestión de tecnologías en sus procesos con el fin de coordinar y liderar la implementación de nuevos servicios y herramientas o la mejora de los mismos para beneficiar directamente a los usuarios.

A través de capacitación en áreas de seguridad y privacidad de la información el proceso de Gestión de TI de la Gobernación de Boyacá evalúa los niveles de satisfacción y uso con el fin de fortalecer su proceso bajo el fundamento de mejora continua y permitir el aprovechamiento óptimo de los recursos (humanos, tecnológicos, de infraestructura y económicos).

Las actividades contenidas en el plan de entrenamiento están dirigidas a los interesados clave y se plantean con el propósito de mitigar riesgos. Para el éxito del cambio; lo que requiere de un despeje adecuado de barreras y la potenciación de habilitadores como hacer uso de canales de comunicación como:

- Correo electrónico.
- Boletines electrónicos (Intranet).
- Reuniones presenciales.
- Redes sociales.
- Campañas visuales.
- Otros (Foros, chats, etc.).

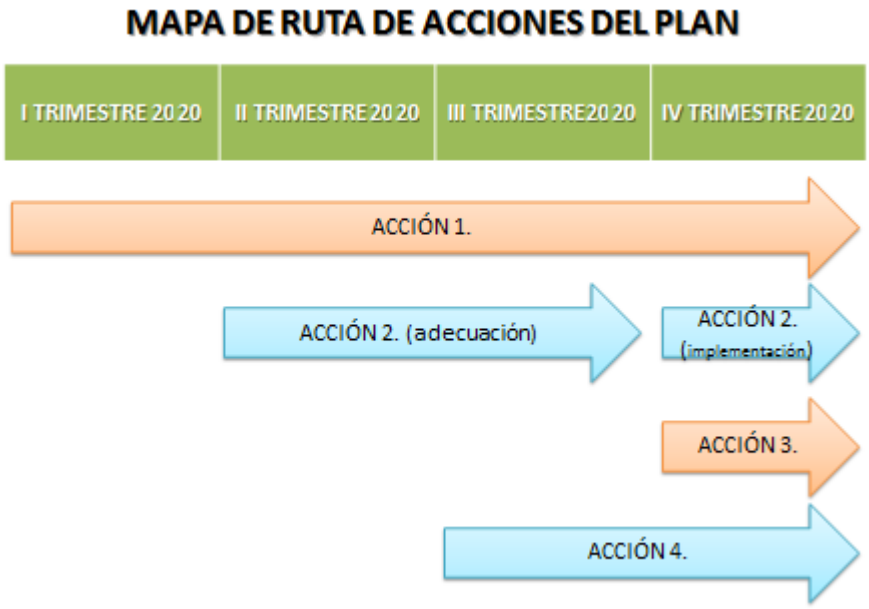
20. ACCIONES DE MEJORA

El sistema integrado de gestión de la Gobernación de Boyacá se encuentra enfocado en el principio de mejora continua de tal manera que todas las acciones realizadas por la Dirección de Sistemas en el proceso de Gestión de TI están enmarcadas de la misma manera en el ciclo **PHVA**.

El plan de Seguridad y Privacidad de la Información contempla las siguientes acciones para el periodo vigente:

- Acción 1. Re potencialización 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.
- Acción 2. Adecuación e implementación de Centro de Procesamiento Alterno (CPA) que permita tener disponible versiones de sistema operativo, plataformas de base de datos, de servicios Web y configuraciones necesarias que estén compatibles y sincronizados con los servidores principales.
- Acción 3. Creación de protocolo de activación del plan y notificación oficial en la Gobernación de Boyacá ante la ocurrencia de un desastre.
- Acción 4. Adecuación de ubicación física para ejecución del plan de recuperación de desastres.

Figura 1. Mapa de ruta de acciones de mejora periodo 2020



Fuente: elaboración propia

21.PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE LA POLÍTICA

Las actividades formuladas en el plan de seguridad y privacidad de la información se pueden observar en el siguiente cronograma:

Tabla 5. Plan de trabajo para el tratamiento de riesgos de seguridad digital

ACTIVIDAD	FASE	2020												2021												2022												MEDICIÓN Y SEGUIMIENTO	
		I CUATRIM				II CUATRIM				III CUATRIM				I CUATRIM				II CUATRIM				III CUATRIM				I CUATRIM				II CUATRIM				III CUATRIM				INDICADOR	% AVANCE
	MESES ===>	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4		
1. Actualización de las políticas de seguridad y privacidad de la información en el manual respectivo por la Dirección de Sistemas de Información	PLANIFICACIÓN																																					Actividades ejecutadas / Actividades programadas	
2. Aplicar el instrumento para el levantamiento y clasificación de activos de información conforme al procedimiento A-AD-TI-P-008	PLANIFICACIÓN																																						
3. Realizar el diagnóstico de seguridad de la información y el análisis del impacto del negocio	PLANIFICACIÓN																																						
4. Establecer la declaración de aplicabilidad	PLANIFICACIÓN																																						
5. Actualización del programa de sensibilización sobre seguridad de la información	PLANIFICACIÓN																																						
6. Implementar el programa de sensibilización sobre seguridad de la información	EJECUCIÓN																																						
7. Implementar la transición del protocolo IPV4 a IPV6	EJECUCIÓN																																						
8. Implementar las actividades según brecha analizada en	EJECUCIÓN																																						

GOBERNACIÓN DE Boyacá	**FORMATO**	**VERSIÓN: 0** **CÓDIGO: A-AD-TI-F-007**
PLAN DE SEGURIDAD DE LA INFORMACIÓN		**FECHA: 26/Ago/2019**

ACTIVIDAD	FASE	2020												2021												2022								MEDICIÓN Y SEGUIMIENTO	
		I CUATRIM				II CUATRIM				III CUATRIM				I CUATRIM				II CUATRIM				III CUATRIM				I CUATRIM				II CUATRIM				III CUATRIM				INDICADOR	% AVANCE
	MESES ===>	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4		
	implementación al modelo MSPI																																						
9.	Monitoreo y revisión de política de seguridad digital por parte de los procesos de la entidad																																					Actividades ejecutadas / Actividades programadas	
10.	Evaluación de política de seguridad digital por parte de oficina asesora de Control interno de gestión	MONITOREO Y REVISIÓN																																					
11.	Formulación del plan de mejoramiento continuo de la política de seguridad	MEJORA																																				Actividades ejecutadas / Actividades programadas	
12.	Ejecución del plan de mejoramiento continuo de la política de seguridad	MEJORA																																					

Fuente: Elaboración propia