CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE CAMBIO**
1	13-10-2017	Creación de la Política de Seguridad y Privacidad de la Información
2	18-02-2019	Se realiza modificación y ajusta documento de acuerdo a los parámetros establecidos en la norma ISO/IEC 27001:2013

CONTROL DEL DOCUMENTO		
ELABORÓ	**REVISÓ**	**APROBÓ**
KATHERINE LIESEL HEREDIA HERNÁNDEZ Profesional de Apoyo Contrato STEPHANIE PÉREZ SIADO Profesional de Apoyo MECI-CALIDAD	MARBY PATRICIA TEJEDOR REYES Miembro MECI-Calidad	DAIMER ALVEIRO PACHECO BAUTISTA Líder Proceso de Gestión de Sistemas

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En la actualidad la información tiene un gran valor económico, estratégico y legal para las entidades, siendo deber de la Gobernación de Casanare resguardar los principios de confidencialidad, integridad y disponibilidades que hacen parte de la seguridad de la información, debido a que estos son un factor indispensable para lograr conseguir los objetivos definidos por la entidad.

La Gobernación de Casanare ha decidido implementar, operar y mejorar de forma continua la Seguridad de la Información de la entidad, soportado en lineamientos claros alineados a las necesidades y requerimientos regulatorios que le aplican a nuestra entidad.

La Política de Seguridad y Privacidad de la Información, es una herramienta institucional que permite sensibilizar a cada uno de sus servidores públicos sin importar su tipo de vinculación al igual que a terceros que presten sus servicios a la Gobernación de Casanare, sobre la importancia y sensibilidad de la información y los servicios que se prestan.

2. OBJETIVO

Brindar directrices y lineamientos necesarios para preservar y fortalecer la confidencialidad, integridad y disponibilidad en temas relacionados con seguridad de la información ante posibles amenazas internas o externas que se presenten en la Gobernación de Casanare.

3. ALCANCE

Aplica a todos los servidores públicos de la entidad sin importar su tipo de vinculación, terceros o usuarios que sean autorizados para interactuar con cualquier activo de la información de la Gobernación de Casanare.

4. NORMA Y O LINEAMIENTOS

- Manual de Gobierno Digital.
- Modelo de Seguridad de la Información para política de Gobierno Digital.
- NORMA TÉCNICA COLOMBIANA ISO/IEC Colombia 27001:2013.
- Ley 734 de 2002, por la cual se expide el código disciplinario único.
- Ley 1273 de 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado-denominado "de la protección de la información y de los datos".
- Decreto 1078 de 2015 Decreto Único Sectorial.
- Decreto Nacional No 1413 de 2017 "Por el cual se adiciona el titulo 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto1072 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales".
- Decreto 1008 de 2018 Política de Gobierno Digital.

5. TÉRMINOS Y DEFINICIONES

Activo de Información: Es todo aquello que en la entidad es considerado importante o de alta validez para la misma ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.

Amenaza: Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

Análisis de riesgos: Uso sistemático de la información para identificar las fuentes y estimar el riesgo NTC-ISO /IEC 27001.

CAD: Centro Administrativo Departamental

CDU: Código Disciplinario Único

Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Copias de respaldo: Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Firewall: Un firewall es un dispositivo de seguridad diseñada para permitir, monitorear, restringir o limitar las conexiones en determinados puertos de comunicación de la red interna o externa, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Incidentes de seguridad de la información: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información.

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

Infraestructura tecnológica: Es el conjunto de hardware y software para el funcionamiento de los diferentes servicios con los que cuenta la entidad.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

MSPI: Modelo de Seguridad y Privacidad de la Información.

No Repudio: Proporciona la prueba ante una tercera parte de que tanto una entidad como una persona han participado en una comunicación.

Política de Seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:20005): intención y dirección general expresada formalmente por la Dirección.

Riesgo: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

Seguridad de la Información: es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

Seguridad perimetral: corresponde a la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos y lógicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles.

Servidor: Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

SGSI: Sistema de Gestión de Seguridad de la información.

Vulnerabilidad: Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

VPN: Virtual Private Network, una red privada virtual que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como internet.

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1 Comité de Seguridad Y Privacidad De La Información - CSPI

La Gobernación de Casanare, creó el Comité de Seguridad y Privacidad de la Información mediante el decreto 0335 de 30 de diciembre de 2015, el cual tiene como objeto apoyar en la coordinación, formulación e implementación del Sistema de Gestión de Seguridad de la Información, está conformado por:

- Secretaría General o su delegado.
- Jefe de la Oficina de Sistemas e Informática o su delegado.
- Director del Departamento Administrativo de Planeación o su delegado.
- Coordinador de MECI – CALIDAD o su delegado.
- Jefe de la Oficina Asesora Jurídica o su delegado.
- Profesional Universitario de Archivo o su delegado.
- Jefe Oficina de Control Interno de la Gestión o su delegado.

El comité se reunirá de manera ordinaria cada 6 meses o de manera extraordinaria cada que las circunstancia lo ameriten, también se podrán reunir por iniciativa de cualquiera de sus integrantes.

6.2 Roles y responsabilidades.

Para efectos de garantizar la funcionalidad de las acciones necesarias para proteger, preservar y administrar la información y las herramientas tecnológicas, es preciso definir los roles y responsabilidades de cada una de las instancias que intervienen, en su desarrollo, implementación y mejoramiento continuo:

6.2.1 El Gobernador de Casanare: Aprobará la política o sus modificaciones, una vez haya sido revisada y aceptadas por el Comité de Seguridad y Privacidad de la Información.

6.2.2 El Comité de Seguridad y Privacidad de la Información: Propondrá y revisará el texto de la política, las funciones generales, la estructuración, recomendación, seguimiento y mejora de la misma.

6.2.3 El Jefe de la Oficina de Sistemas e Informática: En su condición de Líder del Comité de Seguridad y Privacidad de la Información, se encargará de coordinar las acciones e impulsar la implementación y el cumplimiento de la presente política, así como definir estrategias de sensibilización al interior de la entidad.

6.2.4 Secretarios de Despacho, Directores y Jefes de Oficina: Velarán por el cumplimiento de las normas aquí establecidas y mantendrán informada a la Oficina de Sistemas e Informática de los cambios o rotación del personal con el fin de desactivar o reasignar los servicios que tengan asignados.

6.2.5 La Oficina de Control Interno de Gestión: Evaluara que los servidores públicos hayan conocido y estén aplicando en su quehacer institucional, la Política de Seguridad y Privacidad de la Información.

6.2.6 Director de Talento Humano: Velar que todo el personal vinculado en carrera administrativa, provisionalidad, libre nombramiento – remoción y contratistas de sus obligaciones con respecto al cumplimiento de la Política de Seguridad y Privacidad de la Información.

6.2.7 Jefe de la Oficina Asesora Jurídica: Asesorará en materia legal a la entidad en temas relacionados con la seguridad y privacidad de la información.

6.2.8 Administradores o Responsables de Activos de Información: Secretarios de Despacho o jefes de dependencia que tengan a cargo Sistemas de información, mantendrán la integridad y confidencialidad de la información que allí se maneje, mientras sea utilizado por usuarios internos o externos. Como también definirán qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

La Dirección de Talento Humano y la Oficina de Sistemas e Informática realizarán socialización y capacitaciones a todo el personal en cuanto a las Políticas de Seguridad y Privacidad de la Información.

Todos los usuarios externos e internos de la Gobernación de Casanare, que previamente hayan sido autorizados para acceder a los recursos tecnológicos y de procesamiento de información de la Entidad, son responsables del cumplimiento de las políticas, procedimientos y normatividad vigente definida por la misma.

6.3 Principios en Seguridad de la Información

A continuación se establecen 12 principios de seguridad que soportan el SGSI de la Gobernación de Casanare:

- Se ha decidido definir, implementar, operar y mejorar de forma continua la seguridad de la información de la entidad, soportado en lineamientos claros alineados a las necesidades y requerimientos regulatorios que le aplican a nuestra entidad.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas y publicadas, y a su vez deben ser acatadas por todos los servidores públicos y terceros.
- Se protegerá la información generada, procesada o resguardada por los procesos de la entidad, al igual que los activos de información que hacen parte de los mismos.
- La Gobernación de Casanare protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La Gobernación de Casanare protegerá su información de las amenazas originadas por parte de los servidores públicos, terceros y personal externo.
- La Gobernación de Casanare protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La Gobernación de Casanare controlará la operación de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Gobernación de Casanare implementará control de acceso a la información, sistemas y recursos de red.
- La Gobernación de Casanare garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Gobernación de Casanare garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La Gobernación de Casanare garantizará la disponibilidad de sus procesos y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La Gobernación de Casanare garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la Política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

7. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Gobernación de Casanare se compromete a otorgar los recursos necesarios para garantizar los tres (3) pilares fundamentales de la Seguridad como son: la disponibilidad, integridad y confidencialidad, con el fin de dar cumplimiento a los objetivos institucionales, la estrategia y misión de la entidad. La Gobernación de Casanare contará con las siguientes políticas generales para ayudar a salvaguardar la información en nuestra entidad:

- La entidad conformará con el Comité de Seguridad y Privacidad de la Información, el cual será encargado de generar recomendaciones para la formulación y adecuación de las políticas, planes programas y proyectos en temas relacionados con seguridad de la información.

- La Oficina de Control Interno deberá, dentro de su programa de auditoría, evaluar que la entidad y las dependencias hayan tomado acciones para fortalecer temas de seguridad de la información.

- Toda contratación relacionada con la TIC en temas como: Adquisición de infraestructura tecnológica, aplicaciones informáticas, software entre otros debe llevar un aval del jefe de la Oficina de Sistemas e Informática en el componente técnico del estudio previo.

- La Oficina de Sistemas e Informática validara que el software suministrado a los equipos tecnológicos se encuentre debidamente licenciado y actualizados.

- Todos los servidores públicos y contratistas serán responsables por el buen uso de la información y la infraestructura tecnológica al igual que el de reportar incidentes o amenazas que puedan causar daño o riesgo a dichos activos.

- La Gobernación de Casanare debe optar por contar siempre con un firewall o dispositivo de seguridad perimetral que permita restringir el acceso no autorizado salvaguardando la información en la entidad.

- Los Jefes de dependencia velarán por el correcto manejo de la información y la infraestructura tecnológica de su personal dentro de su dependencia con el fin de cumplir con lo establecido en las Políticas de Seguridad y Privacidad de la Información de la Gobernación de Casanare.

- La Oficina de Sistemas e Informática, fomentarán cultura y buenas prácticas en el manejo de la información, entre los servidores públicos, contratistas y terceros con el fin de conservar la integridad en temas de información.

- Todos los servidores públicos que cuenten con medios de comunicación escrito como correo institucional o chat, deberán garantizar que su participación es personal e intransferible en una comunicación al momento de emitir o recibir la información, esto se conoce como: no repudio.

Adicionalmente, la Gobernación de Casanare contara con las siguientes políticas específicas para el conocimiento de los servidores públicos:

8. SEGURIDAD DE LOS RECURSOS HUMANOS.

La Dirección de Talento Humano con apoyo de la Oficina Asesora Jurídica deberá comprobar los antecedentes al igual que los estudios realizados por las personas que aspiran a un cargo en la entidad de acuerdo a las leyes, normas y códigos éticos que apliquen para tal caso.

La Dirección de Talento Humano deberá velar para que el perfil del personal a ingresar este acorde a las responsabilidades y funciones del cargo para el cual aplicara.

Cada Jefe de dependencia debe promover la lectura de la Política de Seguridad y Privacidad de la Información a los contratistas que se vinculen a su área de trabajo.

Los servidores públicos y contratistas deben recibir capacitación de la Política de Seguridad de la Información y socialización en buenas prácticas con el fin de poder mitigar riesgos o pérdida de la información.

Todo funcionario sin importar su tipo de vinculación, será sujeto disciplinable, según lo definido por la ley, por acciones, omisión, incumplimiento o desacato a la Política de Seguridad y Privacidad de la Información.

Cada Jefe de dependencia deberá reportar a la Oficina de Sistemas e Informática los cambios del personal sea por traslados o cambio de actividades con el fin de poder actualizar o desactivar los servicios tecnológicos que posean.

9. GESTIÓN DE ACTIVOS

9.1 Responsabilidades y uso sobre los activos

La Gobernación de Casanare será el propietario de la información que se procese, produzca o almacene dentro de la entidad por los servidores públicos o contratistas.

La Gobernación de Casanare mantendrá un inventario actualizado de sus activos de información, el cual será administrado por el Almacén Departamental y la Oficina de Sistemas e Informática, dichos activos estarán claramente identificados y definidos para el conocimiento del personal autorizado.

Cada jefe de dependencia brindara al Almacén Departamental y a la Oficina de Sistemas e Informática, el apoyo necesario con el fin de recopilar información que permita la actualización del inventario de los activos de información.

Los servidores públicos y contratistas solo utilizaran el software y hardware autorizados por la Oficina de Sistemas e Informática.

La Oficina de Sistemas e Informática realizara la revisión de los programas (software) utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considerada como una violación a la Política de Seguridad y Privacidad de la Información de la Gobernación de Casanare.

Todos los responsables de los procesos de la Gobernación de Casanare deben generar un análisis de riesgos en temas de seguridad de la información, con el fin de ser unificado y dado a conocer a la Oficina de Sistemas e Informática, para la búsqueda soluciones que pueda mitigar dichos riesgos.

Cuando se requiera de aplicativos, sistemas de información y equipos informáticos deben ser solicitados a la oficina de sistemas con su correspondiente justificación, con el fin de validar su posible viabilidad.

La Oficina de Sistemas e Informática será quien custodie el software, manuales y licencias de uso de los equipos informáticos, sistemas de información o aplicativos.

No está permitido por parte de los servidores públicos instalar, modificar o copiar software al igual que extraer o instalar hardware de los equipos de la Gobernación de Casanare, sin previa autorización o supervisión de la Oficina de Sistemas e Informática.

Los usuarios en cabeza de los jefes de dependencia deben informar a la Oficina de Sistemas e Informática sobre cualquier anomalía, violación o incidente que evidencien en contra de los activos de información.

Las acciones que se generen dentro de las cuentas de usuario, serán responsabilidad únicamente del funcionario al cual esté vinculada dicha cuenta.

Todo funcionario desvinculado o trasladado deberá hacer entrega de los activos de información tanto físicos como magnéticos al jefe de dependencia. Al igual que dejar documentado lo realizado durante su estadía laboral.

Las dependencias de la Gobernación de Casanare deberán realizar el inventario de activos de información correspondiente de acuerdo a los parámetros estipulados en el Anexo 1. GU-SS-01: Gestión y clasificación de activos de información V. 01, esta información deberá ser reportada a la Oficina de Sistemas e Informática.

La Oficina de Sistemas e Informática realizará la consolidación y publicación del inventario de activos de información de acuerdo a la información suministrada por cada una de las dependencias.

10. CONTROL DE ACCESO

10.1 Requisitos para control de acceso a redes y servicios en red.

Para el acceso a los servicios tecnológicos (sistemas de información, aplicativos, ingreso al equipo, entre otros), la Oficina de Sistemas e Informática suministrará a los servidores públicos, previamente autorizados por sus Jefes de dependencias, el usuario y una contraseña de acceso, ésta última debe ser cambiada en el primer ingreso.

Todos los usuarios y contraseñas son personales e intransferibles, ningún funcionario deberá ingresar a los servicios tecnológicos que preste la Gobernación de Casanare, con usuarios distintos a los asignados por la Oficina de Sistemas e Informática, lo cual se tipifica como suplantación de identidad y constituye incumplimiento a las Políticas de Seguridad de la Información.

Todos los servidores públicos que deba ingresar hardware propio a las instalaciones del CAD, para el cumplimiento de sus actividades deberán solicitar por medio del Jefe de Dependencia la autorización para conectarse a la red de la Entidad. Dicha solicitud se realizara a la Oficina de Sistemas e Informática quienes validaran la disponibilidad y autorizaran la conexión.

Todo dispositivo hardware propio que no cuente con autorización de la Oficina de Sistemas e Informática para conectarse a la red interna del CAD, entrara en un proceso de suspensión del servicio, mientras se realice la respectiva solicitud.

La conexión remota a la red de área local de la Gobernación de Casanare debe realizarse a través de una conexión VPN segura suministrada por la entidad y autorizada por la Oficina de Sistemas e Informática.
La creación y modificación de usuarios en los sistemas de información deben ser solicitadas por medio escrito por parte del Jefe de Dependencia que lo requiera.

No es permitida la utilización de herramientas, software, dispositivos o aplicaciones que anule o evite controles de seguridad informática aplicados por la entidad.

10.2 Gestión de acceso de usuarios.

La Oficina de Sistema e Informática solicitara el acta de inicio de los contratistas como requisito para creación de cualquier recurso tecnológico que requiera usuario y contraseña, con el fin de tener la fecha de finalización y así retirar los derechos de acceso a los contratistas que hayan culminado su vinculación laboral.

Los Jefes de dependencia debe informar a la Oficina de Sistemas e Informática cuando un funcionario o contratista ya no administre o interactúe algún recurso tecnológico, con el fin realizar la desactivación de los permisos.

Se establece el uso de contraseñas individuales para determinar las responsabilidades de cada funcionario en la administración de los diferentes recursos tecnológicos a su cargo. Todo documento que vincule a una persona para trabajar en la Gobernación de Casanare debe menciona un compromiso de no divulgación de la información de la entidad, creando así un acuerdo de confidencialidad del funcionario con la entidad.

Los usuarios pueden elegir cambiar sus contraseñas de acceso periódicamente, inclusive antes de que estas expiren, teniendo en cuenta las siguientes recomendaciones: deben contener mayúsculas, minúsculas, números y por lo menos un carácter especial, siendo la longitud mayor a 8 caracteres.

Los usuarios no deben utilizar ninguna estructura o característica de contraseña que pueda dar como resultado una contraseña predecible o deducible con facilidad, evitar digitar palabras de un diccionario, secuencias de caracteres comunes, detalles personales o cualquier parte gramatical.

El sistema solicitara cada 45 días el cambio obligatorio de la contraseña.

Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministrada por la Oficina de Sistemas e Informática.

Se debe evitar la reutilización de las contraseñas anteriores.

La Oficina de Sistemas e Informática deberá cambiar todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware (por ejemplo: impresoras, routers, switch, herramientas de seguridad, entre otras).

La contraseña de acceso asignada por la Oficina de Sistemas e Informática no se debe prestar, divulgar o difundir a compañeros, jefes u otras personas que lo soliciten.

Todos los servidores públicos, sin importar su tipo de vinculación, serán responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.

Las contraseñas no deben ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.

Los usuarios finales no deben configurar, instalar y eliminar software de los equipos de cómputo de la Gobernación de Casanare, la interfaz del sistema operativo debe estar configurada de tal forma que tenga solo privilegios de invitado. Todas estas labores deben ser estrictamente realizadas por la Oficina de Sistemas e Informática.

11. CONTROLES CRIPTOGRÁFICOS.

La Oficina de Sistema e Informática, asegura el uso apropiado de los datos enviados a través de internet por medio del correo corporativo, aplicación Contractvs, aplicación de impuesto a vehículos, sitio web institucional www.casanare.gov.co; aplicación PQRSD, por medio de la autenticación, encriptación y desencriptación, para proteger la confiabilidad, la autenticidad y/o la integridad de la información.

12. SEGURIDAD FÍSICA Y AMBIENTAL

12.1 Áreas seguras.

La Dirección de Servicios Administrativos identificará las áreas o dependencias que procesan o almacenan información sensible o crítica, con el fin de fortalecer controles, para evitar el ingreso a personal no autorizado.

La Dirección de Servicios Administrativos instalará y realizará mantenimiento a los dispositivos con los que cuente cada área o dependencia segura de la entidad.

La Dirección de Servicios Administrativos con apoyo de la Oficina de Sistemas e Informática en los casos que lo amerite configurarán e instalarán los dispositivos para el ingreso a áreas seguras tales como: (sensores, cámaras, biométricos, entre otros).

Todas las entradas que utilizan sistemas de control de acceso (biométricos) deben permanecer cerradas, en caso de ser abiertas los servidores públicos deberán cerrarlas.

Todo personal sin importar su tipo de vinculación debe tener y portar su carnet en un lugar visible mientras permanezcan dentro de las instalaciones de la entidad.

El centro de datos deberá contar como mínimo con las siguientes características:

- Controles de acceso y seguridad física
- Controles de humedad y temperatura
- Sistemas eléctricos regulados y respaldos de energía
- Aire acondicionado redundante para en caso de falla exista respaldo
- Bajo riesgo de inundaciones
- Alarmas de detección de humo y sistemas automáticos de extinción de fuego
- Extintores de incendio para fuego generado por equipos eléctricos.

Sólo ingresará de manera frecuente al centro de datos el personal autorizado por el Jefe de la Oficina de Sistemas e Informática, los cuales realizan actividades frecuentes y tendrán para tal fin registrado su huella para la lectura en el biométrico.

El personal interno o externo que no cuente con registro dactilar, debe ser autorizado por el Jefe de la Oficina de Sistemas e Informática para poder ingresar al Centro de Datos y a su vez debe registrarse en el formato control de acceso a áreas restringidas FO-SS-10.

En el centro de datos está prohibido mantener papelería y materiales que representen riesgo de propagación de fuego.

Es deber de los servidores públicos informar sobre falencia en temas de seguridad física que evidencien dentro de la entidad, dándolos a conocer a la Dirección de Servicios Administrativos.
Las actividades de soporte, mantenimiento o limpieza dentro del centro de datos siempre deben ser supervisadas por personal del área de sistemas e informática.

Las instalaciones de la entidad deben estar dotadas de un circuito cerrado de TV con el fin de monitorear y registrar las actividades de Servidores públicos, contratistas y visitantes.

12.2 Controles de acceso físico.

Las áreas seguras, dentro de las cuales se encuentran el centro de datos, centros de cableado, áreas de archivo, áreas de recepción, entrega de correspondencia y demás definidas por la Dirección de Servicios Administrativos, deben contar con mecanismos de protección física, ambiental y controles de acceso adecuados para la protección de la información.

En las áreas seguras, bajo ninguna circunstancia se puede fumar, o consumir alimentos.

Las actividades de limpieza en las áreas seguras deben ser supervisadas por un Servidores públicos o Colaboradores del proceso. El personal de limpieza se debe capacitar acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.

12.3 Seguridad de los equipos.

La ubicación de los equipos de cómputo de la gobernación de Casanare debe ser en áreas de trabajo que permitan la seguridad de los mismos, evitando el ingreso de personal no autorizado y riesgos ambientales como humedad, goteras o exceso de polvo.

Los equipos de cómputo deberán ser conectados a una red regulada de energía con el fin de protegerlos de picos de luz o fallas en el suministro de luz.

La Dirección de Servicios Administrativos y la Oficina de Sistemas e Informática realizara revisiones periódicas al cableado tanto eléctrico como de datos respectivamente, con el fin de mantener el normal funcionamiento de los servicios evitando interferencias o fallos.

La Dirección de Servicios Administrativos deberá asegurar un respaldo de energía automático en caso de falta de suministro de energía en periodos cortos o largos, que permitan tomar acciones para salvaguardar los servicios prestados por la entidad.

La Oficina de Sistemas e Informática programara mantenimiento preventivo en los equipos de cómputo de toda la entidad con el fin de preservar el normal funcionamiento de los computadores así como la integridad y disponibilidad de la información que allí se encuentra.

Solo servidores públicos designados por la Oficina de Sistemas e Informática estarán autorizados para instalar software o hardware en los equipos, servidores e infraestructura tecnológica de la Gobernación de Casanare.

No se podrá realizar actividad alguna de tipo remoto en equipos o servidores de la entidad sin la debida autorización de la Oficina de Sistemas e Informática de la Gobernación de Casanare la cual se reserva el derecho de asignación según considere.

El personal de la entidad no podrá acceder a las áreas de procesamiento o almacenamiento de información ni a los lugares donde se estén ubicado equipos hardware que hagan parte de la infraestructura tecnológica que soporten a los sistemas de información, sin previa autorización de quien corresponda.

Los equipos de cómputo al que se les preste mantenimiento preventivo o correctivo deberá ser registrado mediante el formato solicitud de soporte FO-SS-01, elaborado por el técnico o profesional que realice el mantenimiento.

Ningún equipo de cómputo perteneciente a la entidad podrá ser retirado de las instalaciones de la Gobernación de Casanare, sin la autorización previa del Jefe de Dirección de Servicios Administrativos y visto bueno del Jefe de la Oficina de Sistemas e Informática, esto con el fin de velar por la información que se encuentre almacenada.

El ingreso y salida de hardware o recursos tecnológicos como portátiles, impresoras, escáneres entre otros, deberá ser controlado por la Dirección de Servicios Administrativos y la conexión de los mismos a la red interna de la entidad deberán tener la autorización de la Oficina de Sistemas e Informática.

Es responsabilidad de los servidores públicos dejar bloqueados los equipos de cómputo en momentos de ausencia laboral durante su jornada de trabajo, con el fin de salvaguardar la información de la entidad.

El escritorio virtual de cada equipo de cómputo independiente del sistema operativo que use, debe mantenerte despejado, no debe contener archivos de ningún tipo salvo los accesos directos a aplicaciones necesarias en la labor del empleado.

Es deber de los servidores públicos cerrar los aplicativos y servicios de red cuando no los estén utilizando.

Al imprimir documentos de carácter confidencial o información sensible, estos deben ser retirados de la impresora inmediatamente.

12.4 Gestión de medios removibles.

Las dependencias de la entidad, deben cumplir con la estrategia de soporte para reducir las probabilidades de contagio de virus a través de los medios removibles, realizadas por la Oficina de Sistemas e Informática.

13. SEGURIDAD DE LAS OPERACIONES

13.1 Procedimientos y responsabilidades de operación.

Los procesos operativos de la Oficina de Sistemas e Información y las operaciones correctas y seguras de las instalaciones del centro de procesamiento de datos ubicado en el cuarto piso, torre A, del Centro Administrativo Departamental, se documentan y se ponen a disposición de todos los usuarios por medio del Anexo 2. MA-SS-01: Manual de operaciones técnicas V. 02.

La Oficina de Sistemas e Informática documentará los diferentes servicios operativos relacionados con tecnologías de la información y las comunicaciones con el fin de que estén disponibles para los usuarios autorizados que lo requieran.

La Oficina de Sistemas e Informática deberá hacer seguimiento a los recursos informáticos con el fin de ajustarlos aprovechando el máximo rendimiento de los sistemas en un futuro.

13.2 Protección contra software malicioso.

La infraestructura de TI está compuesta por activos. Un activo o recurso informático, se define como todo aquello pueda generar valor para la empresa u organización y que éstas sientan la necesidad de proteger. Un activo está representado por los objetos físicos (hardware, routers, switches, hubs, firewalls, antenas, computadoras), objetos abstractos (software, sistemas de información, bases de datos, sistemas operativos) e incluso el personal de trabajo y las localidades físicas.

Estos activos están propensos a amenazas, las cuales son aquellas que representan un peligro para los activos o a la seguridad de la información en general, las cuales pueden ser perpetuadas internamente o externamente.

La presencia observada de software malicioso en los servidores ponen en riesgo la confidencialidad e integridad de la información almacenada en ellos, para contrarrestar esto, la Oficina de Sistemas e Informática cuenta con software de protección (Antivirus) contra software malicioso y con un dispositivo firewall para la seguridad perimetral.

La Oficina de Sistemas e Informática realizará una capacitación y/o campaña de concientización anual a los funcionarios sobre la seguridad de la información, buscando reducir el uso indebido que los funcionarios tienen sobre sus propias credenciales, adicional la Oficina de Sistemas e Informática cuenta con un directorio activo (Active Directory), que permite la gestión de los permisos de acceso en los diferentes servicios otorgados por el personal de la Oficina de Sistemas e Informática.

13.3 Copias de respaldo.

Los servidores públicos y contratistas de cada dependencia, serán los responsables de hacer las copias de respaldo de información en el equipo de cómputo asignado para el cumplimiento de sus funciones contractuales.

La Oficina de Sistemas e Informática debe hacer copias de respaldo de la información, software y sistemas de información almacenados en los servidores del centro de datos, con los cuales se cuente con la administración y ponerlos a prueba regularmente.

Para la información software y sistemas de información alojados dentro de servidores externos o servidores internos, en donde la Oficina de Sistemas e Informática no cuente con la administración, es responsabilidad de la dependencia responsable, el cumplimiento de las copias de respaldo periódicas y sus respectivas pruebas.

13.4 Registro y seguimiento.

La Oficina de Sistemas e Informática velará por la sincronización de los relojes de todos los sistemas de procesamiento pertenecientes a la entidad, almacenados en el centro de datos y con los cuales la dependencia cuente con su administración, se encuentren referenciadas con una única fuente de referencia de tiempo.

Los Jefes de las dependencias velarán por la sincronización de los relojes de todos los sistemas de procesamiento pertenecientes a la entidad, con los cuales la dependencia cuente con su administración, se encuentren referenciadas con la fuente de referencia de tiempo determinada por la Oficina de Sistemas e Informática.

13.5 Gestión de vulnerabilidad técnica.

Las dependencias de la entidad, deben reportar oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen, a la Oficina de Sistemas e Informática.

La Oficina de Sistemas e Informática dentro de su proceso de Gestión de Sistemas, deberá evaluar la exposición de la organización a las vulnerabilidades detectadas dentro de la matriz de riesgos tecnológicos y tomar las medidas apropiadas para el tratamiento del riesgo asociado, garantizando la continuidad de las operaciones de los usuarios de los sistemas tecnológicos y de información de la entidad.

La Oficina de Sistemas e Informática cuenta con restricciones sobre la instalación de software, ya que sólo puede ser realizada por personal autorizado con software libre y/o licenciado.

13.6 Monitoreo

La Gobernación de Casanare busca establecer mediciones necesarias para calificar la operación y efectividad de los controles, estableciendo niveles de cumplimiento y de protección de los principios de seguridad y privacidad de la información.

La Oficina de Sistemas e Informática, define y realiza actividades que conduzcan a la evaluación, monitoreo y direccionamiento de los resultados de los servicios TI para apoyar los procesos internos de la institución.

Se trabaja continuamente para la inclusión de las dependencias en la identificación de áreas con oportunidad de mejora, de acuerdo con los criterios de calidad establecidos en el Modelo Integrado de Planeación y Gestión de la institución, de modo que se pueda focalizar esfuerzos en el mejoramiento de los procesos de TI para contribuir con el cumplimiento de las metas institucionales y

14. SEGURIDAD DE LAS COMUNICACIONES

14.1 Gestión de seguridad de las redes

La Oficina de Sistemas e Informática es la responsable de administrar y gestionar la red de datos de la entidad y de establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.

La entidad proporciona en la medida de lo posible a los Servidores públicos y terceros los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales, por lo cual no es permitido conectar a puntos de acceso de la red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por la Oficina de Sistemas e Informática de la Gobernación de Casanare.

La entidad debe establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información.

Se deben establecer parámetros técnicos para la conexión segura de la red con los servicios de red.

Se deben establecer mecanismos de autenticación seguros para el acceso a la red.

14.2 Transferencia de información

La Gobernación de Casanare asegurará la protección de la información en el momento de ser transferida o intercambiada de forma interna mediante cada una de sus dependencias o de forma externa con otras entidades y entes descentralizados, para lo cual establecerán Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. La administración Departamental propenderá por el uso de tecnologías de la información y las comunicaciones para llevar a cabo el intercambio de información.

15. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

15.1 Requisitos de seguridad de los sistemas de información

Todas las dependencias que adquiera, desarrollen o establezcan contratos de soporte para los sistemas de información debe contar con aprobación en el componente técnico por parte de la Oficina de Sistemas.

15.2 Seguridad en los procesos de desarrollo y soporte

Todas las dependencias de la Gobernación de Casanare deben incluir dentro de los contratos de desarrollo o soporte, el documento denominado anexo de contrato para desarrollo de software seguro, elaborado por la Oficina de Sistemas e Informática, que sirve como guía para estandarizar la seguridad en los procesos de desarrollo y soporte de la entidad.

16. RELACIONES CON LOS PROVEEDORES

16.1 Seguridad de la información en las relaciones con los proveedores

La Dirección de Servicios Administrativos deberá asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

La Oficina de Sistemas e Informática deberá asegurar la protección de los activos del centro de datos que sean accesibles a los proveedores.

La entidad deberá establecer e implementar una política de seguridad de la información para las relaciones con los proveedores, que permita proteger los activos de la entidad.

17. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información de la entidad.

Todo incidente ocurrido dentro de las dependencias de la entidad debe ser registrado y enviado al correo *soporte@casanare.gov.co* con evidencia que soporte el evento.

La Oficina de Sistemas e Informática por medio del FO-SS-01 Solicitud Soporte Sistemas, realizará el registro del incidente de seguridad por medio del formato de indicadores FO-SS-06 Informe Mensual de Servicios Prestados, y evidenciará el reporte al Colcert (Grupo de respuesta a emergencias cibernéticas de Colombia).

Se debe dar tratamiento adecuado a los incidentes de seguridad de la información que sean reportados por las dependencias de la entidad.

Todos los Servidores públicos sin importar su tipo de vinculación tienen la responsabilidad de reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la Seguridad de la información que detecten en la entidad al correo soporte@casanare.gov.co.

Se debe documentar los incidentes que sean tratados y solucionados, creando una ayuda para el tratamiento de nuevos incidentes.

18. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

La alta gerencia velará por la inclusión de requisitos para la seguridad de la información en situaciones adversas estipuladas como riesgos en la entidad, dentro de plan de continuidad del negocio de la organización.

19. CUMPLIMIENTO

19.1 Cumplimiento de los requisitos legales y contractuales

Los diferentes aspectos contemplados en esta Política de Seguridad y Privacidad de la Información son de obligatorio cumplimiento para todos los servidores públicos de la Gobernación de Casanare sin importar su tipo de vinculación. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, La Oficina Asesora Jurídica tomará las acciones disciplinarias y legales correspondientes.

La Política de Seguridad y Privacidad de la Información se realiza con el fin de dar a conocer a todos los servidores públicos los responsables y las tareas de cada uno en

temas de seguridad de la información, evitando así incumpliendo a los controles de seguridad de la información que debe tener la entidad.

Los Secretarios, directores y jefes de oficina velarán por el cumplimiento del Anexo 3. Circular 001 de 24 de agosto 2016: Políticas de operación del proceso de gestión de sistemas, la cual establece *"Toda contratación relacionada con las TIC, será previamente analizada por la OSI, teniendo que estar plasmada en el plan anual de sistemas y/o llevando el aval del jefe de la OSI en el componente técnico del estudio previo".*

19.2 Propiedad Intelectual

La Gobernación de Casanare será la propietaria de todos y cada uno de los derechos patrimoniales de cualquier software (código fuente y base de datos), desarrollado a solicitud de la entidad.

Los terceros que contraten desarrollo software con la entidad, deberán entregar certificado, constancia o contrato de cesión de todos y cada uno de los derechos patrimoniales a favor de la Gobernación de Casanare, a partir de la fecha de entrega de la aplicación.

19.3 Revisiones de seguridad de la información

Los secretarios, directores y jefes de dependencias velaran por supervisar el cumplimiento de las políticas por parte de sus servidores públicos en sus respectivas dependencias.

La Oficina de Control Interno de Gestión: Evaluara periódicamente que los servidores públicos cumplan con las políticas de seguridad de la información establecidas.
La Oficina de Sistemas e Informática realizara revisiones esporádicas para corroborar que los servidores públicos cumplan con lo relacionado en seguridad de la información en áreas sensibles para la entidad.

20. INCUMPLIMIENTO

El Código Disciplinario Único, Ley 734 de 2002, establece en su Artículo 34, que son deberes de los servidores públicos, entre otros, los siguientes en los numerales 4, 5 y 7:

Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.

Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función, conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.

Cumplir las disposiciones que sus superiores jerárquicos adopten en ejercicio de sus atribuciones, siempre que no sean contrarías a la Constitución Nacional y a las leyes vigentes, y atender los requerimientos y citaciones de las autoridades competentes.

Así mismo la referida norma señala en su Art. 48, numeral 16, 43; que constituye falta gravísima:

Atentar, con cualquier propósito, contra la inviolabilidad de la correspondencia y demás formas de comunicación, u obtener información o recaudar prueba con desconocimiento de los derechos y garantías constitucionales y legales.

Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas.

Consecuentemente menciona el CDU, en el Artículo 50, que constituye Faltas graves y leves, el incumplimiento de los deberes, el abuso de los derechos, la extralimitación de las funciones, o la violación al régimen de prohibiciones, impedimentos, inhabilidades, incompatibilidades o conflicto de intereses consagrados en la Constitución o en la ley.

21. ANEXOS

Anexo 1. GU-SS-01: Gestión y clasificación de activos de información V. 01.
Anexo 2. MA-SS-01: Manual de operaciones técnicas V. 02.
Anexo 3. Circular 001 de 24 de agosto 2016: Políticas de operación del proceso de gestión de sistemas.
Anexo 4. FO-SS-06 Informe Mensual de Servicios Prestados.
Anexo 5. FO-SS-01 Solicitud Soporte Sistemas.