ALCALDÍA DE CAJICÁ

MANUAL DE POLÍTICAS DE SEGURIDAD PARA SITIOS WEB

DIRECCIÓN DE TICS-CTeI

2020

Calle 2 No. 4-07 - Cajicá - Cundinamarca - Colombia
Código postal: 250240 PBX (57+1) 8795356 - 8837077
Correo: contactenos-pqrs@cajica.gov.co Página web: www.cajica.gov.co

CO-SC-CER-701118

CONTENIDO

CONTENIDO	2
INTRODUCCIÓN	3
PRESENTACIÓN DEL MANUAL	3
1.1 Objetivo de Manual	3
1.2 Alcance del Manual de Normas de Seguridad de la Información	3
2. TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN	3
3. NORMAS DE SEGURIDAD DE LA INFORMACIÓN	5
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	5
3.1 Roles y responsabilidades para la seguridad de la información	5
3.2. Separación de deberes	11
3.3. Sensibilización	12
3.4. Perfiles de Acceso	13
3.5. Acceso Controlado a Terceros sobre Recursos Tecnológicos	15
3.6. Monitoreo	16
3.7. Tratamiento de Incidentes de Seguridad	17
3.8. Separación de Ambientes y Funciones	18
3.9. Software Adquirido	19
3.10. Utilización de claves de Acceso	20
3.11. Perfiles de Acceso. Políticas Relacionadas	21
3.12. Protección de Hardware y Software de Seguridad	22
3.13. Copias de Respaldo de Software y Datos de Seguridad	23
3.14. Cifrado de Datos	24
3.15. Integridad de la Información	25
3.16. Prevención y Detección de Virus	27
3.17. Respaldo de Información	28
3.18. Seguridad de las comunicaciones	29
3.19. Seguridad Física - Dispositivos de Seguridad Contra Incidencias	32
3.20. Seguridad Física –Backups	33
3.21. Gestión de Incidentes de Seguridad de la Información Responsabilidades y Procedimientos	33

3.22. Reporte de eventos de seguridad de la información	35
3.23. Disponibilidad de instalaciones de procesamiento de información	36
3.24. Gestión de la Prestación de Servicios de Proveedores. Política de Gestión de Proveedores	37
3.25. Cumplimiento de los requisitos legales. Protección de datos personales	38
REFERENCIAS BIBLIOGRÁFICAS	40

La base del presente documento es el Manual de Políticas de Seguridad de la Información, el cual contiene los lineamientos en términos de seguridad definidos por **ALCALDÍA DE CAJICÁ**.

Dichos lineamientos fueron desarrollados de acuerdo a los requerimientos propios de la empresa para contrarrestar los riesgos que se puedan presentar en cualquier eventualidad en la prestación de nuestros servicios con cada uno de nuestros clientes.

Por otra parte, en el presente documento de Manual de Normas de Seguridad de la Información se establecen las acciones concretas a tomar para materializar el cumplimiento de las políticas definidas en el Manual de Políticas de Seguridad de la Información. De acuerdo a la definición y objetivo de cada una de las Normas que se definirán a continuación, estas pueden hacer el desarrollo de una o más políticas de seguridad. De la misma forma una política de seguridad puede ser desarrollada a través de varias normas de seguridad.

1. PRESENTACIÓN DEL MANUAL

1.1. Objetivo de Manual

El presente Manual, tiene por objeto establecer las acciones que se deben ejecutar al interior de **ALCALDÍA DE CAJICÁ** para dar cumplimiento a las políticas de Seguridad de la Información. Estas acciones se expresan mediante imperativos, procedimientos y guías que definen el tratamiento de los riesgos detectados y que a su vez permiten brindar un servicio de calidad a nuestros clientes tanto en entidades privadas como públicas.

1.2. Alcance del Manual de Normas de Seguridad de la Información

El presente Manual de Normas de Seguridad de la Información es parte integral de todos los procesos en **ALCALDÍA DE CAJICÁ** y es de obligatorio cumplimiento por parte de todos los funcionarios y demás colaboradores de la empresa.

2. TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN

Los siguientes términos y definiciones están basados en el estándar y son aplicables a **ALCALDÍA DE CAJICÁ**:

Aceptación de riesgo: Decisión de asumir un riesgo.

Activo: Cualquier elemento que represente valor para la organización.

Alta Dirección: Se considera Alta Dirección a los directivos con cargo más alto en una organización; el Presidente, el Gerente General y los Directores de las distintas áreas. En el caso de **ALCALDÍA DE CAJICÁ** se entiende como Alta Dirección a la integrada por el representante legal.

Análisis de Riesgo: Uso sistemático de la información para identificar fuentes y para estimar el riesgo.

Adaptabilidad: Define que todos los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Comité de Seguridad de la Información: El Comité de Seguridad de la Información, es un cuerpo integrado por representantes designados por la Alta Dirección con el objetivo de garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

Confiabilidad de la Información: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, empresas o procesos no autorizados.

Declaración de aplicabilidad: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una empresa.

Dueño del riesgo sobre el activo: Persona o empresa con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Información: Datos que poseen una información.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Calle 2 No. 4-07 - Cajicá - Cundinamarca - Colombia
Código postal: 250240 PBX (57+1) 8795356 - 8837077
Correo: contactenos-pqrs@cajica.gov.co Página web: www.cajica.gov.co
CO-SC-CER-701118

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad d la información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Política: actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos.

Procedimiento: Forma especificada de llevar a cabo una actividad o un proceso.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

Recursos informáticos: Todos aquellos componentes de hardware y programas (software) que son necesarios para el buen funcionamiento y la optimación del trabajo con computadores y periféricos, tanto a nivel Individual, como colectivo u organizativo, sin dejar de lado el buen funcionamiento de los mismos.

Registro: Documento que presenta resultados obtenidos o proporcionar evidencia de actividades desempeñadas.

Responsable de Seguridad TIC: En LA EMPRESA el comité de seguridad de la información será el grupo encargado de realizar el seguimiento y monitoreo al Sistema de Gestión de la Seguridad de la información (SGSI).

Responsables del Activo: Personas responsables del activo de información en el proceso.

Riesgo: El efecto de la incertidumbre sobre los objetivos". (Icontec, 2011, Pág.4)

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: Nivel restante de riesgo después del tratamiento del riesgo.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

Sistema de gestión de la seguridad de la información SGSI: Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales que se realicen en la empresa.

Tecnología de la Información: Se refiere al hardware y software operado por el organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la empresa.

Tratamiento del riesgo: Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

3. NORMAS DE SEGURIDAD DE LA INFORMACIÓN

Una norma de la seguridad de la información sustenta una política de seguridad y regula parte o la totalidad del objetivo de la misma.

Actualización de Normas

Cualquier solicitud de modificación al documento de Normas de Seguridad de la Información **ALCALDÍA DE CAJICÁ**, debe ser realizada por el Comité de Seguridad de la Información.

Estructura de la Norma

La estructura de la Norma es la siguiente:

- Título de la norma
- Políticas relacionadas
- Objetivo
- Alcance
- Descripción

Reglas de escritura de las Normas

Las normas se escribirán en forma sencilla y en su texto indicarán que es una definición
general y aplicable a la empresa.

El enunciado debe ser corto, bien redactado y conciso, además se utilizarán términos y palabras que sean de uso común.

Se mantendrán los términos de seguridad TIC definidos y expresados dentro del documento de seguridad de **ALCALDÍA DE CAJICÁ**.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

3.1. Roles y responsabilidades para la seguridad de la información

Políticas Relacionadas: Organización interna de la seguridad de la información, Terminación de contrato o cambio de responsabilidad en el empleo, Propiedad de los activos, Uso aceptable de los activos, Devolución de activos, Responsabilidades y procedimientos.

Objetivo: Definir las responsabilidades para la seguridad de la información que tienen las diferentes áreas dentro del Sistema de Gestión de Seguridad de la Información **ALCALDÍA DE CAJICÁ**.

Alcance: Esta norma deberá ser adoptada por todos los colaboradores de **ALCALDÍA DE CAJICÁ** que intervienen dentro del Sistema de Gestión de Seguridad de la Información de la empresa.

Descripción:

Responsabilidades

A continuación se presentan las responsabilidades de los principales elementos que intervienen en la construcción del Sistema de Gestión de Seguridad de la Información:

1. Responsabilidades de la Alta Dirección

La alta dirección debe promover el compromiso de todos los niveles de responsabilidad y autoridad de **ALCALDÍA DE CAJICÁ** en la implementación de Sistema de Gestión de Seguridad de la Información. Para ello tiene las siguientes funciones específicas:

- Velar por el establecimiento de las políticas de seguridad de la

información y los objetivos de seguridad alineados con las necesidades **ALCALDÍA DE CAJICÁ**.

- Garantizar la integración de los lineamientos del SGSI con los procesos definidos en **ALCALDÍA DE CAJICÁ**.

- Comunicar la necesidad de definir y mantener una gestión de la seguridad de la información representada por medio de los objetivos y las políticas de seguridad.

- Apoyar y promover a las personas para que contribuyan al desarrollo del SGSI y adquieran un rol de liderazgo en cada una de sus áreas de responsabilidad.

- Garantizar los recursos requeridos para el mantenimiento del SGSI.

Responsabilidades de la Oficina TIC ALCALDÍA DE CAJICÁ

Es responsabilidad de la Oficina de TIC de la empresa:

- Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de seguridad de información.
- Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de seguridad de información.
- Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de seguridad de la información.
- Diseñar, desarrollar, instalar y mantener las aplicaciones bajo su responsabilidad de acuerdo con la metodología establecida e incluyendo los controles de seguridad de información.
- Establecer, documentar y dar mantenimiento a los procedimientos de seguridad que apliquen para la plataforma de tecnologías de información administrada por esta oficina.
- Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.
- Establecer y dar mantenimiento a los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.
- Supervisar los procesos y/o actividades sobre las plataformas tecnológicas que manejen información de **ALCALDÍA DE CAJICÁ** y cuya administración se encuentre delegada en tercero.
- Implementar y administrar los controles de seguridad sobre los datos y conexiones de la red bajo su administración.
- Definir y gestionar programas de capacitación y entrenamiento que incluyan

temas relevantes y pertinentes sobre seguridad de información.

- Custodiar la información y los medios de almacenamiento bajo su responsabilidad.

Responsabilidades de Gestión de riesgos de Seguridad de la Información

Es responsabilidad de la Oficina Administrativa, con el apoyo del Oficial de Seguridad de la Información, llevar a cabo la Gestión de Riesgos de Seguridad de la Información en **ALCALDÍA DE CAJICÁ** en concordancia con las políticas de seguridad y sus objetivos.

El objetivo de la Gestión de riesgos es identificar y evaluar los riesgos de seguridad de la información a los cuales están expuestos los activos de la empresa, para seleccionar y aplicar el plan de tratamiento más adecuado. La evaluación de riesgos está basada en el impacto y probabilidad de ocurrencia de estos para la empresa y los requerimientos de los niveles de seguridad, tomando en cuenta los controles existentes.

El análisis y evaluación de riesgos de seguridad debe hacerse al menos una vez al año.

Es responsabilidad de los propietarios del riesgo:

- Clasificar sus activos de información de acuerdo con los requerimientos de confidencialidad, integridad y disponibilidad.
- Definir los requerimientos de continuidad y de recuperación en caso de desastre.
- Realizar un análisis anual de riesgos, para determinar el grado de exposición a las amenazas vigentes y confirmar los requerimientos de confidencialidad, integridad y disponibilidad relacionados con sus activos de Información
- Definir los requerimientos de seguridad con el acompañamiento del Oficial de Seguridad, para los activos de información bajo su responsabilidad para que se les proporcione un nivel adecuado de protección en conformidad con los estándares, políticas y procedimientos de seguridad de información.
- Determinar y autorizar todos los privilegios de acceso a sus activos de información.
- Comunicar y gestionar al Oficial de Seguridad de la Información sus requerimientos en capacitación sobre seguridad de información.
- Definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados a su proceso, incluyendo aquellas actividades que sean consideradas como controles de seguridad de la información dentro de dichos procedimientos.

Responsabilidades de funcionarios, contratistas y terceros

Es responsabilidad de los colaboradores (Funcionarios y Contratistas) y Terceros salvaguardar la información institucional de la empresa, garantizando así la confidencialidad, integridad y disponibilidad de la información teniendo como

funciones:

- Cumplir fielmente las políticas y normas de seguridad de la información, contempladas en el presente manual.
- Reportar, a la mayor brevedad posible y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de seguridad de información.
- Realizar sugerencias a la Alta Dirección para mejorar los procesos relacionados con los activos de información de la empresa y optimizar así el sistema de seguridad de la información.
- Utilizar los sistemas de información y el acceso a la red únicamente para los propósitos indicados en las políticas de seguridad de la información.
- Incorporar la seguridad de información como parte de las actividades y tareas bajo su responsabilidad.

- Conocer las directrices de protección de los activos de información descritas en los manuales de políticas y normas de seguridad de la información.
- Utilizar únicamente software y demás recursos tecnológicos autorizados por la empresa.

Cláusulas aplicables a contratistas y terceros

Se debe coordinar con la Secretaria General y con la Oficina Asesora Jurídica la inclusión en los procesos de contratación las cláusulas de confidencialidad e integridad definidas en la presente norma, correspondientes a salvaguardar la confidencialidad e integridad de los activos de información **ALCALDÍA DE CAJICÁ**.

En los contratos que establezca **ALCALDÍA DE CAJICÁ** se deberán agregar las siguientes cláusulas:

- Cláusula de Confidencialidad de la Información: El Contratista se compromete a mantener la reserva de la información privilegiada y protegida que se le suministre y a no revelar tal información a terceras personas. Esto aplica adicionalmente al Tratamiento de Datos Personales antes, durante y después del contrato. En caso de incumplimiento de esta cláusula, se ejecutará la normatividad aplicable, incluidas la Ley 734 de 2002 y la Ley 1273 de 2009.

- Cláusula de Integridad de la Información: El Contratista o Tercero debe conocer y aceptar las condiciones definas en la norma, descrita en el presenta documento, las cuales se refieren al manejo íntegro e integral de la información tanto interna como externa. Toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios

correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.

3.2. Separación de deberes

Políticas Relacionadas: Organización interna de la seguridad de la información, Separación de los ambientes de desarrollo, de pruebas y operación, Separación de redes.

Objetivo: Realizar la correcta distribución de roles y responsabilidades, atendiendo a la debida segregación de funciones para reducir las oportunidades de una modificación no- autorizada y mal uso (intencional o no-intencional) de los activos de la organización.

Alcance: Esta norma define la manera de realizar la separación de deberes, roles o responsabilidades de los diferentes cargos en **ALCALDÍA DE CAJICÁ**, para empleados y contratistas o terceros.

Descripción: Cada área o dependencia de la empresa de manera autónoma e independiente de otras áreas, considerando que la segregación de los deberes es un método para reducir el riesgo de un mal uso accidental o deliberado del sistema, tiene el compromiso de que:

- El Oficial de Seguridad de la Información, en apoyo con el líder del proceso, debe mantener un inventario actualizado de los activos de información de cada área o dependencia y de acuerdo al grado de criticidad de dichos activos, el Oficial de Seguridad de la Información debe determinar la necesidad de realizar una segregación de funciones.
- Se deben identificar los riesgos asociados a modificación no-autorizada y mal uso (intencional o no-intencional) de los activos de información, provocada por una falta de separación de deberes. Dependiendo del nivel de riesgo detectado el Oficial de Seguridad de la Información debe determinar la necesidad de realizar una segregación de funciones.
- En casos en que sea difícil segregar funciones, el Oficial de Seguridad debe considerar otros controles como el monitoreo de actividades y rastros de auditoría.
- Se deben activar y fortalecer los controles establecidos para la gestión efectiva de los riesgos asociados a la separación de deberes, conforme a las determinaciones del Comité de Seguridad.
- Se debe aprobar y dar curso a las acciones de mejora establecidas en el Comité de Seguridad con la finalidad de llevar los riesgos asociados a la separación de funciones hasta los niveles aceptados por la empresa, según los criterios aplicados por el Oficial de Seguridad para **ALCALDÍA DE CAJICÁ**.
- Se debe hacer seguimiento a las acciones de mejora con sus correspondientes controles de seguridad de la información aprobadas por el

Comité de Seguridad, particularmente en lo referente a la separación de deberes.

- Se debe mantener el inventario actualizado de activos de información bajo la dirección del Oficial de Seguridad, de tal forma que se identifiquen aquellos que puedan requerir una separación de deberes.
- A cargo del Oficial de Seguridad, se debe mantener actualizado el análisis de riesgos de seguridad donde se visibilicen aquellos provocados por una falta de separación de deberes, de tal forma que se identifiquen aquellas actividades que puedan requerir dicha separación de deberes.

3.3. Sensibilización.

Políticas Relacionadas: Toma de conciencia, educación y formación en la seguridad de la información.

Objetivo: Que los colaboradores de **ALCALDÍA DE CAJICÁ** reciban una adecuada sensibilización en seguridad de la información y las actualizaciones regulares sobre las políticas y procedimientos establecidos por el SGSI para la empresa conforme sea relevante para su función laboral.

Alcance: Esta norma deberá ser considerada por toda persona que tenga un rol activo en el uso y protección de los activos de información, los cuales incluyen elementos hardware, elementos software, información física, información digital, personas, locaciones, etc. Es decir debe ir dirigida a todos los colaboradores de la empresa.

Descripción:

- Se debe impartir la capacitación y el conocimiento a los colaboradores de **ALCALDÍA DE CAJICÁ** a cargo del Oficial de Seguridad, diseñado para introducir las políticas y expectativas de seguridad de la organización que afecten a **ALCALDÍA DE CAJICÁ**, antes de otorgar acceso a la información o servicios.

- Debe programarse una capacitación constante cuya frecuencia la define el Comité de Seguridad **ALCALDÍA DE CAJICÁ**, la cual debe incluir los requerimientos de seguridad de información y responsabilidades legales, así como la capacitación en el uso correcto de los medios de procesamiento de información como por ejemplo, procedimiento de registro, uso de paquetes de software e información sobre los procesos disciplinarios.

- Las actividades de concientización, lideradas por el Oficial de Seguridad, deben ser adecuadas y relevantes para el rol, responsabilidades y capacidades del colaborador en **ALCALDÍA DE CAJICÁ**. Deben incluir información sobre amenazas conocidas y establecer los canales apropiados para reportar los incidentes de seguridad de la información.

- Con el debido cuidado a los aspectos de confidencialidad según el criterio del Oficial de Seguridad, los incidentes en la seguridad de la información deben ser utilizados en la capacitación de los usuarios como ejemplos de lo que podrían suceder, cómo responder ante tales incidentes y cómo evitarlos en el futuro.

- Cada colaborador de la empresa debe participar de las sesiones de sensibilización sobre Seguridad en la Información, según lo defina la Coordinación de Desarrollo Humano de **ALCALDÍA DE CAJICÁ**.

- Se debe realizar un proceso continuo de talleres de sensibilización en seguridad de la información para todos los colaboradores de la empresa bajo la supervisión del Oficial de Seguridad.

- Se deben hacer periódicamente presentaciones magistrales guiadas por el Oficial de Seguridad, mediante ayudas didácticas de manera que se logre en el público la apropiación de la información presentada y una efectiva generación de conocimiento, mediante la experiencia de hechos cotidianos relacionados con la seguridad de la información **ALCALDÍA DE CAJICÁ**.

- Se debe plantear en las capacitaciones, casos críticos con ejemplos de situaciones reales. Las sesiones de sensibilización deben estar apoyadas en casos prácticos que se evidencian al interior de **ALCALDÍA DE CAJICÁ** y que tengan relación directa con los activos de información más críticos identificados en la empresa.

- Se debe hacer uso de material gráfico, con el apoyo de la Oficina de Comunicaciones **ALCALDÍA DE CAJICÁ**, como posters y fondos de pantalla lo cual aporta a la estrategia de divulgación una mayor capacidad de recordación en los colaboradores **ALCALDÍA DE CAJICÁ**.

3.4. Perfiles de Acceso

Políticas Relacionadas: Privacidad y protección de información de datos personales, Política de control y Administración de accesos, Seguridad para Internet, Seguridad para redes inalámbricas, Administración de cuentas, Gestión de cambios, Control de redes, Seguridad de los servicios de red.

Objetivo: Evitar el acceso no autorizado a los servicios de la red, regulando la creación, asignación, cambios y retiros de perfiles de acceso.

Alcance: Esta norma define la manera en que se crea, otorga, cambia y se inactivan los perfiles de acceso que poseen los colaboradores a los distintos recursos tecnológicos **ALCALDÍA DE CAJICÁ**.

Descripción:

Se debe garantizar el acceso de los usuarios a las redes y los servicios de red sin comprometer la seguridad de la información, para lo cual **ALCALDÍA DE CAJICÁ** debe tener en cuenta los siguientes lineamientos técnicos:

- Se deben aplicar los mecanismos AAA (Authentication, Authorization and Accounting), apropiados para todos los colaboradores de **ALCALDÍA DE CAJICÁ** que deban ingresar a los ambientes de administración de los dispositivos de comunicaciones o servidores, mediante el uso de aplicaciones como Radius o Tacacs y el Directorio Activo. Es responsabilidad del Oficial de Seguridad el llevar a cabo su implementación con el apoyo del Coordinador de Servicios Tecnológicos.

- Se debe seguir el procedimiento de "Creación y cancelación de cuentas de usuario" de acuerdo a los siguientes lineamientos:
- Los usuarios sólo deben tener acceso a los servicios para los cuales hayan sido específicamente autorizados.
- El procedimiento de creación y cancelación de cuentas de usuario debe tener cobertura a todas las redes y servicios **ALCALDÍA DE CAJICÁ**.

Los mecanismos de autenticación y autorización automática de usuarios para acceso a los servicios de **ALCALDÍA DE CAJICÁ** es responsabilidad del Oficial de Seguridad con el apoyo del Coordinador de Servicios Tecnológicos y debe tener los siguientes lineamientos:

- Las credenciales de autenticación básicas son: nombre de usuario, contraseña y dirección de tarjeta de red del computador. Esto obliga a que el usuario solo ingrese a los sistemas de información desde su equipo de trabajo.
- Las credenciales de los usuarios en lo posible deber ser gestionadas por medio de un Directorio Activo, permitiéndose otros esquemas de acuerdo al criterio del Oficial de Seguridad de la Información.

- Se deben identificar los requerimientos de autenticación y autorización orientados al acceso y uso de las aplicaciones misionales y de apoyo de **ALCALDÍA DE CAJICÁ** de manera individual consultando los fabricantes, proveedores, desarrolladores y/o responsables de estas aplicaciones en la medida de sus niveles de criticidad para la empresa. Esta labor debe estar encabezada por el Oficial de Seguridad con la colaboración del Responsable de Gestión de Proyectos y del Coordinador de Servicios Tecnológicos.
- Se debe tener en cuenta que los perfiles de usuario deben estar ajustados a niveles de privilegio estrictos de acuerdo a los sistemas que use por razones del desempeño de sus funciones de tal manera que no le sea posible ingresar a otros campos de información de la empresa para evitar el incumplimiento

normativo como el habeas data personal, habeas data financiero, la ley de transparencia, etc.

- Se debe revisar de manera periódica en **ALCALDÍA DE CAJICÁ** (cada seis meses), el procedimiento de creación y cancelación de cuentas de usuario con el fin de identificar posibles riesgos, proponer planes de mejoramiento e implementar o reforzar controles de seguridad de la información.
- Las situaciones en las cuales se podrá revocar los derechos de acceso son las siguientes: terminación del contrato de trabajo, uso inadecuado del activo de información y/o traslado del colaborador a otra área de trabajo.
- Es responsabilidad de la oficina encargada de implementar el procedimiento de creación y cancelación de cuentas de usuario, el definir, asignar y mantener actualizados los perfiles de acceso a la información en cada una de las aplicaciones de acuerdo con las funciones del colaborador.
- A partir de la fecha de creación de este documento y con el fin de poder lograr una seguridad homogénea y altamente administrable, los sistemas de información que se desarrollen o adquieran deben diseñarse de forma tal que permita la administración de perfiles.
- Se debe inventariar la totalidad de los usuarios, identificar los servicios y aplicaciones que utilizan, revisar la validez de los permisos actuales de acceso y aplicar los permisos de acuerdo a los criterios de seguridad apropiados según el cargo de cada usuario.

3.5. Acceso Controlado a Terceros sobre Recursos Tecnológicos

Políticas Relacionadas: Seguridad de la información para las relaciones con proveedores, Tratamiento de la seguridad dentro de los acuerdos con proveedores, Privacidad y protección de información de datos personales, Política de control y Administración de accesos, Perímetro de seguridad física, Controles de Accesos Físicos.

Objetivo: Gestionar los riesgos a la información y a las instalaciones de procesamiento de información que existen en los procesos donde se involucra a Terceros, de acuerdo a los requerimientos institucionales y de seguridad para el acceso a los recursos tecnológicos **ALCALDÍA DE CAJICÁ**.

Alcance: Aplica a todas las actividades de acceso a la información de **ALCALDÍA DE CAJICÁ** que involucren a terceros.

Descripción:

Donde exista la necesidad de permitir a una empresa contratista o a un tercero el acceso a las instalaciones de procesamiento de la información o la información **ALCALDÍA DE CAJICÁ**, el Oficial de Seguridad de la Información debe llevar a

cabo una evaluación del riesgo que le permita identificar los controles de seguridad requeridos para proteger la información conforme a la actividad que va a desarrollar el contratista o Tercero. Para esto se deben tener en cuenta los siguientes lineamientos:

- Se deben determinar las instalaciones de procesamiento de información o la información de **ALCALDÍA DE CAJICÁ** a la cual el contratista o Tercero necesita tener acceso.

- Se debe identificar el tipo de acceso que tendrá el contratista o Tercero a la Información y las instalaciones de procesamiento de información:

Acceso físico: Implica acceso directo a las locaciones de **ALCALDÍA DE CAJICÁ**, por ejemplo: oficinas, edificios de cómputo, archivadores.

Acceso lógico: Implica acceso directo a la información digital **ALCALDÍA DE CAJICÁ**, por ejemplo: bases de datos o sistemas de información **ALCALDÍA DE CAJICÁ**.

Conectividad a la red: Implica acceso por medio de equipos conmutadores de red, por ejemplo, conexión permanente local, acceso remoto por canal dedicado, acceso por VPN en teletrabajo, etc.

- Se debe informar al contratista o tercero acerca de los riesgos de seguridad involucrados en el acceso físico, lógico o de conectividad a la red, según corresponda.

- Se debe determinar el nivel de criticidad de la información expuesta ante el contratista o Tercero y su grado de importancia para las operaciones misionales o de apoyo.

- Se debe identificar el personal del Tercero involucrado en el manejo de la información **ALCALDÍA DE CAJICÁ**.

- Se deben conocer los diferentes medios y controles empleados por el tercero cuando almacena, procesa, comunica, comparte e intercambia información.

- Se debe crear una red destinada al uso del personal contratista o tercero de manera que se pueda controlar y monitorear el acceso a otras redes donde se maneja información confidencial para la empresa.

- Se debe estipular en el contrato los requerimientos legales y reguladores y otras obligaciones contractuales asociadas a seguridad de la información para llevar cabo la labor del contratista o tercero. Esto conforme a lo definido en la

norma. Roles y responsabilidades para la seguridad de la información, en la sección de Clausulas aplicables a contratistas y terceros.

3.6. Monitoreo

Políticas Relacionadas: Organización interna de la seguridad de la información, Propiedad de los activos, Registro de eventos, Responsabilidades y procedimientos.

Objetivo: Producir y mantener registros de auditoría de las actividades y eventos de seguridad de la información durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso de modo que se detecten las actividades de procesamiento de información no autorizadas.

Alcance: Esta norma contempla las actividades de monitoreo que incluye la revisión de registros de eventos que se generan durante la ejecución de los procesos en cada servidor, donde se almacenan registros, alarmas o errores, para la toma de acciones preventivas o correctivas.

Descripción:

- Se deben implementar plataformas de monitoreo, bajo el control del Administrador de Red, que permitan hacer seguimiento al comportamiento de la red de comunicaciones, servidores, aplicaciones y usuarios. De esta manera se disminuyen los riesgos que puedan afectar la disponibilidad e integridad de la información.

- Los registros de monitoreo sobre el manejo de la información de **ALCALDÍA DE CAJICÁ** deben ser analizados por el Administrador de los Sistemas de Seguridad y deben incluir, cuando sea relevante, los siguientes elementos como evidencias para su posterior análisis o para reportes de auditoría:

  - Nombres de usuario o IDs.
  - Fechas, horas y detalles de eventos claves; por ejemplo, ingreso y salida.
  - Identificación o ubicación del dispositivo que accede a la información, si es posible.
  - Intentos de acceso fallidos y rechazados al sistema.
  - Intentos de acceso fallidos y rechazados a los datos y otros recursos.
  - Actividades realizadas por el usuario
  - Nivel de privilegio o perfil de usuario.
  - Utilidades y aplicaciones del sistema empleadas.
  - Archivos a los cuales se tuvo acceso y los tipos de acceso.
  - Direcciones y protocolos de la red.

- Adicionalmente se deben tener registros de monitoreo asociados a cambios

en la configuración del sistema, alarmas activadas por el sistema de control de acceso, activación y desactivación de los sistemas de protección como sistemas antivirus y sistemas de detección de intrusiones. El análisis de estos registros debe estar a cargo del Administrador de los Sistemas de Seguridad.

- Dado que los registros de auditoría pueden contener datos personales confidenciales, se deben mantener las medidas de protección de privacidad apropiadas de acuerdo a la Ley 1581 de 2012 sobre Protección de Datos Personales.

- Los administradores del sistema no deben tener permiso para borrar o desactivar los registros de sus propias actividades.

3.7. Tratamiento de Incidentes de Seguridad

Políticas Relacionadas: Toma de conciencia, educación y formación en la seguridad de la información, Uso aceptable de los activos, Responsabilidades y procedimientos, Reporte de eventos de seguridad de la información, Evaluación de eventos de seguridad de la información y decisiones sobre ellos, Aprendizaje obtenido de los incidentes de seguridad de la información, Recolección de evidencia, Implementación de la continuidad de la seguridad de la información.

Objetivo: Asegurar que los eventos y debilidades de la seguridad de la información sean comunicados de manera que permita realizar una acción correctiva oportuna con un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

3.8. Separación de Ambientes y Funciones

Políticas Relacionadas: Organización interna de la seguridad de la información, Gestión de cambios, Separación de redes.

Objetivo: Reducir los riesgos de acceso y manipulación no autorizada a los ambientes de producción **ALCALDÍA DE CAJICÁ**, con el fin de garantizar una operación correcta de las instalaciones de procesamiento de información.

Alcance: Esta norma regula la separación de ambientes que deberá existir en la infraestructura tecnológica a fin de proveer una segregación de funciones.

Descripción:

- Para controlar la seguridad en las redes, el Administrador de Red debe crear dominios de red lógicos separados. En **ALCALDÍA DE CAJICÁ** se deben tener al menos los siguientes dominios o ambientes de red: ambiente de desarrollo,

ambiente de pruebas y ambiente de producción.
Los dominios de red establecidos y su interrelación deben ser configurados por el Administrador de Red de acuerdo a una evaluación del riesgo realizada por el Oficial de Seguridad de la Información y a los requerimientos de seguridad de cada uno de los dominios. Se deben implementar los controles de acceso adecuados a los diferentes dominios de red conforme a los niveles de privilegio de los diferentes usuarios

Se reconocen los siguientes ambientes básicos en la oficina TIC:

- Ambiente de Desarrollo: En este dominio de red se tienen los elementos hardware y software necesarios para que los colaboradores expertos en desarrollo de sistemas de información y demás servicios de apoyo a **ALCALDÍA DE CAJICÁ** realicen sus actividades sin afectar la producción de la empresa.

- Ambiente de Pruebas: Una vez se hace el desarrollo del sistema de información o aplicación, se deben realizar las pruebas correspondientes. En este ambiente se tienen los elementos hardware y software necesarios para realizar las pruebas a los aplicativos o sistemas de información desarrollados internamente por **ALCALDÍA DE CAJICÁ** o contratados a un tercero. Dichas pruebas son necesarias a fin de constatar que los sistemas realizan correcta e integralmente los requerimientos para los que fueron creados. Este debe ser un ambiente estable, con modificaciones o cambios controlados. Para migrar un sistema, módulo o programa de éste ambiente al de producción debe existir una aprobación formal por parte del funcionario responsable del área involucrada en las pruebas, que actúa como cliente de la aplicación o sistema de información y del jefe de la Oficina TIC. Si se requiere, en este ambiente se deben utilizar datos de prueba y nunca datos de producción.

- Ambiente de Producción: Es el ambiente donde se utiliza y transforman los datos **ALCALDÍA DE CAJICÁ**, por lo tanto es el ambiente donde reside la información operativa de la Empresa. No se permite efectuar pruebas sobre este ambiente a excepción de la primera implementación de cada software.

3.9. Software Adquirido

Políticas Relacionadas: Restricciones sobre la instalación y/o actualización de software.

Objetivo: Establecer procedimientos para controlar la instalación de software en los sistemas operativos, y regular la adquisición de cualquier tipo de software para **ALCALDÍA DE CAJICÁ**.

Alcance: Esta norma contempla todo tipo de software a ser adquirido en **ALCALDÍA DE CAJICÁ**: Sistema operacional, bases de datos, software de comunicaciones, utilitarios del sistema, software de seguridad, software de monitoreo, software de oficina y software aplicativo, entre otros.

Descripción:
Para minimizar el riesgo de corrupción de los sistemas operativos, se deben establecer los siguientes lineamientos de acuerdo al Procedimiento de Control de Cambios:

- La actualización del software operacional, aplicaciones y bibliotecas de programas sólo debe ser realizada por el administrador del sistema operativo o el personal de la mesa de ayuda, previa aprobación del director de la oficina TIC.
- El software de las aplicaciones y el sistema operativo sólo se debe implementar después de una prueba extensa y satisfactoria incluyendo: pruebas de utilidad, pruebas de seguridad, impacto sobre los sistemas de información y facilidad para el usuario. Estas validaciones deben estar supervisadas por el Responsable de la Planeación y Ejecución de Pruebas apoyado por la Mesa de Ayuda.
- Se debe hace uso de una base de datos del conocimiento donde se depositen todas las licencias, manuales y plantillas de configuración de los diferentes dispositivos de cómputo, desde PCs, servidores, equipos de comunicaciones y de seguridad de manera que se tenga un control y gestión centralizado de todo el software empleado en **ALCALDÍA DE CAJICÁ**. Se debe mantener un inventario actualizado de licencias de software **ALCALDÍA DE CAJICÁ**, como parte de la política Inventario de Activos.
- Se debe establecer una estrategia de "regreso a la situación original" (rollback) antes de implementar los cambios.
- Se debe mantener un registro de auditoría de todas las actualizaciones.
- Para efectos de concientización y divulgación, se deben hacer capacitaciones sobre las restricciones en la instalación de software a nivel de la empresa, conforme a los lineamientos dados en el documento XXX- YYY "PLAN DE DIVULGACIÓN DE SEGURIDAD DE LA INFORMACIÓN".
- Para garantizar conformidad con los estándares de seguridad de información propios, se debe adquirir hardware y software a través de canales autorizados, para lo cual se deben tener identificados dichos canales.

Todo el software de la Empresa debe ser legalmente adquirido y se debe contar con las respectivas licencias que lo demuestren.

- Está prohibido para los empleados de **ALCALDÍA DE CAJICÁ** descargar y/o instalar cualquier tipo de software. Todas las solicitudes de instalación o configuración de software deben ser dirigidas hacia la mesa de ayuda de la empresa.
- Todo software a instalarse en las estaciones de trabajo debe estar licenciado.

3.10. Utilización de claves de Acceso

Políticas Relacionadas: Política de control y Administración de accesos, Política

de Gestión de contraseñas, Política sobre el uso de controles criptográficos (Protección de la Información), Gestión de llaves.

Objetivo: Que el manejo de claves secretas en **ALCALDÍA DE CAJICÁ** se realice de forma automatizada, se creen claves secretas adecuadas para la seguridad de la empresa y se regule el uso y características de las claves de acceso.

Alcance: Esta norma define todos los parámetros genéricos que deben poseer las claves de acceso y el mantenimiento que los clientes internos deben llevar a cabo con las mismas.

Descripción:

- Un sistema de gestión de claves secretas debe cumplir con los siguientes lineamientos:

- Hacer uso de IDs de usuarios individuales y claves secretas para establecer responsabilidades.
- El directorio activo no debe permitir repetir claves y debe obligar cambio de primer ingreso automáticamente.
- Permitir a los usuarios seleccionar y cambiar sus propias claves secretas e incluir un procedimiento de confirmación para permitir errores de input.
- La clave secreta debe ser robusta: longitud mínima de ocho caracteres, combinar mayúsculas, minúsculas, números y símbolos. No se deben utilizar palabras sencillas en cualquier idioma, nombres propios, lugares, combinaciones excesivamente cortas, fechas de nacimiento, etc.
- La clave secreta se debe cambiar al menos cada tres meses, para lo cual el sistema debe forzar su caducidad.
- Obligar a los usuarios a cambiar las claves secretas temporales en su primer ingreso o registro.
- Mantener un registro de claves de usuario previas y evitar el re-uso, al menos de 10 contraseñas.
- No mostrar las claves secretas en la pantalla en el momento de ingresarlas.
- Almacenar los archivos de claves secretas separadamente de los datos del sistema de gestión de claves **ALCALDÍA DE CAJICÁ**.
-
- Almacenar y transmitir las claves secretas en un formato protegido (por ejemplo, cifrado).

- La contraseña es privada, confidencial e intransferible, siendo su titular responsable de evitar su divulgación. Ante la presunción de que otra persona pudiera conocer su contraseña, debe proceder a cambiarla inmediatamente. Se considerará causa grave y será sancionado de acuerdo al Código Disciplinario Único (Ley 734 como se describe en la Norma 001 del presente documento), el

hecho de revelar a otra persona su propia contraseña o solicitar la contraseña de otro usuario.

- Se deben modificar todas las contraseñas que traen los equipos (Hardware y Software) por defecto una vez estos se hayan instalados

3.11. Perfiles de Acceso. Políticas Relacionadas:

Objetivo: Regular la definición, instalación y mantenimiento de los parámetros de seguridad de la infraestructura tecnológica **ALCALDÍA DE CAJICÁ**.

Alcance: Esta norma contempla todos aquellos parámetros relacionados directa o indirectamente con la seguridad de la infraestructura tecnológica de la Empresa.

Descripción:

- La homologación de hardware o software a instalar en la Empresa, permite que este sea incorporado respetando los estándares establecidos, logrando de esta forma homogeneidad en los parámetros relativos a la seguridad, permitiendo un control de la infraestructura tecnológica, la facilidad de mantenimiento y monitoreo.
- La Oficina de TIC es la responsable de la homologación del hardware y software mediante un proceso de revisión de los parámetros de seguridad vigentes.
- Es responsabilidad de la Oficina de TIC de la mantener actualizado el manual de estándares de seguridad cuando se incorpore una nueva tecnología.
- Para modificar los estándares establecidos, se debe justificar técnicamente la necesidad, determinar el alcance de la modificación y evaluar el impacto desde el punto de vista de seguridad, con el fin de determinar si debe ser acompañado por otras medidas. Posteriormente y en caso de ejecutarse la modificación, debe registrarse en el formato de control de cambios e implementarse las medidas pertinentes sobre todos los equipos de idénticas características.

3.12. Protección de Hardware y Software de Seguridad

Políticas Relacionadas: Uso aceptable de los activos, Gestión de contraseñas, Separación de los ambientes de desarrollo, de pruebas y operación, Registro de eventos, Protección de la información de registro, Restricciones sobre la instalación y/o actualización de software, Seguridad de los servicios de red.

Objetivo: Regular la protección del hardware y software de seguridad.

Alcance: Esta norma abarca a cualquier hardware y software que se utilice exclusivamente para la seguridad de cualquier ambiente, infraestructura, o

sistema instalado en **ALCALDÍA DE CAJICÁ**, ya sea adquirido o de desarrollo propio.

Descripción: Cualquier hardware y software que sea utilizado exclusivamente con fines de seguridad y control, independientemente de su naturaleza, complejidad o modo de adquisición, debe cumplir las siguientes reglas:

- Los activos que hagan parte del hardware y software de seguridad en **ALCALDÍA DE CAJICÁ**,, deberán estar a cargo de un responsable, que será el Oficial de Seguridad de la Información quien a su vez delegará la custodia y gestión al administrador de los sistemas de seguridad.
- Cualquier uso indebido o mal funcionamiento del Hardware y Software de seguridad en **ALCALDÍA DE CAJICÁ** deberá ser reportado inmediatamente por cualquier usuario dentro de la organización siguiendo el procedimiento de gestión de incidentes.
- Las credenciales de acceso a la gestión del Hardware o Software de seguridad sólo deben ser manejadas por el administrador de los sistemas de seguridad, y por ningún motivo serán divulgadas a terceros, teniendo en cuenta la Política de Gestión de contraseñas.
- El Oficial de Seguridad de la Información debe definir, y el administrador de los sistemas de seguridad debe implementar y gestionar, los elementos de hardware y software de seguridad que garanticen la separación de ambientes de desarrollo, pruebas y operación, teniendo en cuenta el Procedimiento de paso de ambientes de desarrollo y pruebas a ambientes de producción.
- Los registros de eventos provenientes del hardware y el software de seguridad **ALCALDÍA DE CAJICÁ**, deberán conservarse en un lugar seguro con acceso restringido al personal autorizado y con protección de acceso.
- El software de seguridad debe ser utilizado exclusivamente para la Entidad pública o privada en la cual se tenga el contrato.
- No se podrá desactivar, modificar, instalar versiones diferentes, ni realizar ninguna otra actividad que modifique el comportamiento del hardware y software de seguridad, con la expresa autorización del Oficial de Seguridad de la Información y la formal supervisión de las actividades de alteración.
- La documentación, manuales y cualquier otro tipo de información técnica sobre su comportamiento deben residir en la Oficina TIC bajo la responsabilidad del Administrador de los Sistemas de Seguridad y/o el Oficial de Seguridad de la Información.
- Ninguna persona podrá transmitir en modo formal o informal, información sobre los parámetros, variables y modo de instalación de alguna herramienta de seguridad.

3.13. Copias de Respaldo de Software y Datos de Seguridad

Políticas Relacionadas: Uso aceptable de los activos, Gestión de cambios,

Gestión de capacidad, Respaldo de información, Registro de eventos, Protección de la información de

registro, transferencia de información, Control de cambios en el sistema, Controles de Acceso Físico.

Objetivo: Regular la toma de respaldos del software y datos de seguridad.

Alcance: Esta norma abarca a cualquier módulo de control de acceso, herramienta y/o software de seguridad y sus archivos de datos.

Descripción: La Oficina de TIC de **ALCALDÍA DE CAJICÁ** definirá, para los sistemas y archivos involucrados en la seguridad, los siguientes aspectos:

- La información contenida en los servidores se respalda de forma periódica, lo cual se determina de acuerdo al nivel de criticidad del activo de información. A mayor nivel de criticidad, el intervalo de tiempo para realizar las copias de respaldo debe ser menor.
- Los medios de las copias de seguridad se almacenan localmente y en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico y videovigilancia.
- Las copias de seguridad son probadas periódicamente para garantizar la integridad de la información almacenada mediante el mecanismo apropiado de recuperación de información.
- Para garantizar que la información de los funcionarios, contratistas y demás terceros autorizados sea respaldada, es responsabilidad de cada uno mantener copia de la información que se maneje en el recurso compartido definido para cada área y/o usuario.
- Los medios de almacenamiento o copias de seguridad del sistema de archivos, o información de la empresa deben ser etiquetados de acuerdo al área de trabajo y al tipo de información que almacenan.
- Las copias de respaldo en los medios de almacenamiento con información crítica son manipuladas única y exclusivamente por el personal autorizado para ejecutar este procedimiento.
- El Oficial de Seguridad de la Información debe definir el esquema de backups adecuado (tipo de backup, frecuencia, medio de almacenamiento, etc.) para la información a respaldar.

3.14. Cifrado de Datos

Políticas Relacionadas: Privacidad y protección de información de datos personales, Política sobre el uso de controles criptográficos (Protección de la Información).

Objetivo: Regular la utilización de los métodos de cifrado de información de la Superintendencia del Subsidio Familiar.

Alcance: Esta norma busca regular la utilización de los métodos de cifrado a utilizarse por
ALCALDÍA DE CAJICÁ en los canales de comunicaciones.

Descripción: Deben utilizarse métodos de cifrado en los casos en que se requiera que la información de **ALCALDÍA DE CAJICÁ** a ser transmitida a través de canales de comunicación, no sea leída o modificada por personas no autorizadas.

El cifrado de documentos puede llevarse a cabo en las siguientes situaciones:

- En la transmisión de información confidencial o reservada de la empresa hacia empresas o personas externas.
- Cuando haya un acuerdo de confidencialidad con otra empresa o persona sobre la información que se va a transmitir.
- Cuando el propietario del riesgo o el Oficial de Seguridad de la Información consideren que se trata de un activo de información critico basado en una valoración de riesgo.

El uso de controles criptográficos puede llevarse a cabo en las siguientes situaciones:

- Cuando se busque un mecanismo de trazabilidad de las acciones sobre la información de **ALCALDÍA DE CAJICÁ**(creación, recepción, entrega, etc.).
- Cuando se establezca la necesidad de implementar procesos de intercambio electrónico de información con garantía de “no repudio”.

Se definen los siguientes lineamientos para la administración de controles criptográficos:

- Siempre se deben proteger los equipos de cómputo utilizados para la operación de los controles criptográficos, especialmente en los casos de generación, validación y revocación de llaves criptográficas.
- El Oficial de Seguridad de la Información debe identificar los equipos de cómputo en los cuales se realiza procesamiento de información cifrada y establecer los mecanismos de protección adecuados para garantizar la confianza en los controles criptográficos.
- En los casos en los que se realice un proceso de cifrado de la partición del sistema operativo o de todo el disco duro se debe crear un disco de recuperación (Rescue Disk) que permita restaurar el disco cifrado en caso de que se dañe el gestor de arranque, la llave maestra o el sistema operativo. Esto no evita la

necesidad de poseer la correcta contraseña para el descifrado.

- En caso de pérdida de información cifrada, el usuario debe reportar tal situación como un incidente de seguridad de la información mediante el documento Procedimiento de Gestión de Incidentes. De esta forma el Oficial de Seguridad de la Información evaluará si existe un medio (por ejemplo un disco de recuperación) para hacer la recuperación de la información.
- La gestión de llaves o contraseñas asociadas a cualquier usuario de red o de sistema de información debe llevarse a cabo, cuando sea posible, utilizando la arquitectura de directorio activo existente en **ALCALDÍA DE CAJICÁ**. Esto implica que en la medida de lo posible la autenticación, de los usuarios debe hacerse contra el directorio activo. De esta forma se evita manejar bases de datos de contraseñas dispersas y no gestionadas.
- La generación y almacenamiento de claves para el caso de usuarios nuevos debe ser definida en el documento Procedimiento de Creación y cancelación de cuentas de usuario.
- La administración de claves para el caso de usuarios existentes, por ejemplo en situaciones de cambio de claves, se debe resolver mediante una solicitud de soporte incluida en el documento Procedimiento de Soporte y Atención a Solicitudes.

3.15. Integridad de la Información

Políticas Relacionadas: Clasificación de la información, Propiedad de los activos, Seguridad de los servicios de red, Transferencia de la información, Acuerdos sobre transferencia de información, Mensajería electrónica.

Objetivo: Regular la definición y alcance de los controles que garanticen la integridad de la información.

Alcance: Esta norma contempla todos los equipos de cómputo que procesen información **ALCALDÍA DE CAJICÁ**, sean o no de su propiedad y la información transmitida de una fuente a otra con o sin procesamiento.

Descripción:

Se establecen los siguientes apartados tendientes a preservar la integridad de la información **ALCALDÍA DE CAJICÁ**:

- Con el fin de garantizar la integridad de la información por parte de los colaboradores **ALCALDÍA DE CAJICÁ**, se debe establecer un compromiso para el manejo integro de la información interna y externa que se debe incluir en los contratos mediante una cláusula de integridad de la información.

- El Oficial de Seguridad de la Información deberá apoyar la generación de la

cláusula de integridad de la información en conjunto con la Oficina Asesora Jurídica, y realizar las actualizaciones correspondientes en función de las necesidades **ALCALDÍA DE CAJICÁ**.

- Con el fin de garantizar la integridad de la información de **ALCALDÍA DE CAJICÁ**, esta debe ser transferida interna y externamente por medio de los canales oficiales establecidos por la Oficina TIC, especialmente aquellos establecidos para la mensajería electrónica y la transferencia de grandes volúmenes de datos.

- La información de **ALCALDÍA DE CAJICÁ** debe ser entregada de forma íntegra y coherente únicamente a las personas a quien esta va dirigida. Igualmente la modificación de la información de **ALCALDÍA DE CAJICÁ** solo se permitirá bajo autorización del propietario o

responsable de dicha información. Generalmente el propietario de la información es el líder del proceso en el cual la información es generada o custodiada.

- El Oficial de Seguridad de la Información debe definir los controles de seguridad necesarios a implementar para garantizar la integridad de la información en cualquiera de sus estados: En uso (por parte del usuario final o por parte de un proceso en un servidor), en movimiento (en tránsito en la red LAN o WAN) o en reposo (cuando esta almacenada).

Adicionalmente se definen los siguientes controles de seguridad a implementar:

- Revisión del ingreso de información: Todo sistema o programa, debe poseer los controles necesarios que garanticen que la información se ingrese en su totalidad de forma precisa, completa y de acuerdo con los tiempos establecidos.

- Revisión del procesamiento de la información: Todo sistema o programa, debe poseer los controles necesarios que garanticen que la información es procesada en su totalidad de forma completa, exacta y en el período estipulado.

- Autenticación: En los sistemas que procesan, transmiten o gestionan información se deben implementar mecanismos de autenticación de usuario o procesos con el fin de identificar adecuadamente al actor que manipula la información **ALCALDÍA DE CAJICÁ**.

- Autorización: En los sistemas que procesan, transmiten o gestionan información se deben implementar mecanismos de autorización de usuario o procesos con el fin de asegurar que las actividades de manipulación de la información se encuentran autorizadas.

3.16. Prevención y Detección de Virus

Políticas Relacionadas: Controles contra códigos maliciosos.

Objetivo: Minimizar la pérdida de datos y software a través del ataque de virus informático.

Alcance: Esta norma abarca todo el software de la infraestructura tecnológica y aplicaciones de **ALCALDÍA DE CAJICÁ** susceptibles de ser atacados por virus informáticos.

Descripción:

En la infraestructura tecnológica que contenga sistemas operativos o aplicaciones, deben implantarse soluciones que detecten y neutralicen ataques provocados por códigos maliciosos. Para ello se deben tener en cuenta los siguientes lineamientos:

- Se debe configurar una regla general para todas las estaciones de trabajo, equipos portátiles y equipos servidores que evite la descarga de cualquier archivo ejecutable. El Oficial de Seguridad de la Información determinará los equipos exentos de esta regla considerando algunas funciones propias de **ALCALDÍA DE CAJICÁ** que sobre estos se desarrollen por ejemplo: equipos en los que se haga desarrollo, instalación o pruebas de software.

- En la medida de lo posible se debe configurar y desplegar una solución que regule la ejecución de aplicaciones en estaciones de trabajo, equipos portátiles y equipos servidores a aquellas que se encuentran dentro un inventario de aplicaciones autorizadas por la EMPRESA. Si no se dispone de una herramienta de validación automática, se debe auditar de forma regular los equipos de **ALCALDÍA DE CAJICÁ** para corroborar el cumplimiento de este punto.

- Se debe configurar la actualización periódica del conjunto de aplicativos dispuestos contra códigos maliciosos, lo cual incluye la actualización del 40 software así como de los datos requeridos por el software para poder operar tales como base de datos de virus o firmas.

- Se debe configurar la ejecución periódica de un proceso de búsqueda (Scanning) de código malicioso intensivo en los equipos en los cuales se tenga desplegada una solución de virus.

- El Oficial de Seguridad de la Información determinará la necesidad de instalar software contra códigos maliciosos en equipos celulares, dado que estos coenen información relevante de la empresa, especialmente aquellos que contengan el buzón de correo corporativo.

- El Oficial de Seguridad de la Información debe velar porque se lleve a cabo un proceso regular de actualización de parches de seguridad en los sistemas de información **ALCALDÍA DE CAJICÁ**.

- El Oficial de Seguridad de la Información debe revisar periódicamente el conjunto de software instalado en los equipos de procesamiento de información que sustentan los procesos críticos **ALCALDÍA DE CAJICÁ**, identificando la presencia de virus o modificaciones no autorizadas en los mismos.

- Se deben configurar las soluciones contra códigos maliciosos instaladas para verificar la presencia de virus en archivos recibidos de fuentes externas o a través de redes no confiables.

- El Oficial de Seguridad de la Información, con apoyo del Jefe de la Oficina TIC, debe liderar un proceso de concientización a los colaboradores de **ALCALDÍA DE CAJICÁ** en la adopción de diferentes actitudes preventivas frente a virus informáticos que eviten un daño hacia la Empresa, entre ellas verificar el remitente de la información antes de abrirla o ejecutarla.

3.17. Respaldo de Información

Políticas Relacionadas: Inventario de activos, Propiedad de los activos, Política de control y Administración de accesos, Respaldo de la información.

Objetivo: Garantizar que la información de la ENTIDAD sea respaldada en un medio confiable y que sea recuperable cuando se necesite.

Alcance: Esta norma contempla todo tipo de información manejada por los colaboradores de **ALCALDÍA DE CAJICÁ** entre las cuales están:

- Datos de las aplicaciones.
- Sistemas de información (programas fuentes y objetos).
- Software de la infraestructura tecnológica.
- Información Técnica.
- Información contenida en los servidores.
- Bases de Datos.

Descripción:

- El Oficial de Seguridad de la Información debe definir el esquema de los backups de la información **ALCALDÍA DE CAJICÁ**, considerando, la frecuencia de backup, el tamaño de la información, la criticidad otorgada, el medio de almacenamiento, entre otros aspectos relacionados:
  - La información valorada con una disponibilidad o integridad alta, de

acuerdo a la metodología para la identificación de activos deberá tener copias de seguridad, diaria incremental, semanal total y mensual total.

- La información valorada con una disponibilidad o integridad media, de acuerdo a la metodología para la identificación de activos deberá tener copias de seguridad, semanal total y mensual total.
- La información valorada con una disponibilidad o integridad baja de acuerdo a la metodología para la identificación de activos deberá tener copias de seguridad mensual total.

• El custodio de la información es el encargado de hacer el respaldo de información, siguiendo el procedimiento XXX de Copias de Respaldo.

• Todos los respaldos de información tienen la misma criticidad de los activos a respaldar. Por lo tanto, ese valor de criticidad es el que define el esquema de backups a aplicar de acuerdo a lo definido en el punto inicial descrito en la presente norma.

• Se debe registrar en detalle todas las copias de respaldo a la información de **ALCALDÍA DE CAJICÁ** que se ejecutan actualmente, indicando el tipo, la periodicidad, la fecha
de creación y el periodo de retención, teniendo en cuenta el procedimiento de ejecución de backups.

• Todos los respaldos de información deben ser retenidos de acuerdo a lo establecido por las tablas de retención documental y la regulación correspondiente, y deben ser almacenados en un sitio seguro que garantice su confidencialidad, integridad y disponibilidad.

• Es responsabilidad del Oficial de Seguridad de la Información, validar que se realice un respaldo de pruebas cada tres meses, el cual se realiza seleccionando aleatoriamente uno de los respaldos de información que se encuentran registrados.

3.18. Seguridad de las comunicaciones

Accesos Remotos

Políticas Relacionadas: Uso aceptable de los activos, Política de control y Administración de accesos, Seguridad para Internet, Administración de cuentas, Política de Gestión de contraseñas, Política sobre el uso de controles criptográficos (Protección de la Información), Seguridad de los servicios de red.

Objetivo: Especificar el uso de accesos remotos a los recursos informáticos e información **ALCALDÍA DE CAJICÁ**.

Alcance: Esta norma contempla todos los accesos remotos que se establezcan con la Red Interna **ALCALDÍA DE CAJICÁ**.

Descripción:

- La autorización de todo acceso remoto que se necesite realizar a los recursos informáticos de la Superintendencia del Subsidio Familia se otorgará siguiendo el procedimiento de creación y cancelación de cuentas de usuario y tendrá que ser previamente autorizado por el Oficial de Seguridad de la Información.
- Los usuarios que utilicen accesos remotos deberán hacer uso del mismo únicamente para el propósito al cual fue concedido. Por ningún motivo se podrá acceder a información o sistemas diferentes a los solicitados y autorizados según el procedimiento de creación y cancelación de cuentas de usuario.
- Los parámetros y las credenciales de acceso de los usuarios que se utilizarán en los accesos remotos deberán ser suministrados por el administrador de los sistemas de seguridad.
- El Oficial de Seguridad de la Información deberá evaluar previamente la viabilidad del acceso remoto al recurso informático teniendo en cuenta la criticidad del activo y los factores que puedan afectar la seguridad de la conexión.
- Por ningún motivo se deberán compartir las credenciales de acceso remoto asignadas para una conexión, con otro usuario o tercero según lo manifiesta la 012

Política de Gestión de contraseñas.

- Las conexiones realizadas a través del protocolo RDP deberán utilizar mecanismos de cifrado adecuados conforme al documento XXX Guía de Clasificación y Rotulación de la Información y usar mecanismos de autenticación NLA (Network Layer Authecation).
- El Oficial de Seguridad de la Información deberá implementar seguridad perimetral como firewall, IDS, IPS destinados a proteger las conexiones de acceso remoto.
- El Oficial de Seguridad de la Información deberá implementar a todas las conexiones túneles VPN para cualquier acceso remoto.

3.18. Seguridad Internet

Políticas Relacionadas: Uso aceptable de los activos, Seguridad para Internet, Controles contra códigos maliciosos, Seguridad de los servicios de red

Objetivo: Definir los aspectos de seguridad que debe aplicar **ALCALDÍA DE CAJICÁ** para la protección de la información de la Empresa en el uso del servicio de Internet.

Alcance: Esta norma contempla cualquier tipo de comunicación que se establezca a través del servicio de Internet por parte de los colaboradores de la

empresa desde equipos pertenecientes a la Red interna para la realización de tareas operativas.

Descripción: Para el acceso a Internet, los funcionarios, contratistas y demás personas que hagan uso del servicio, deben tener en cuenta los siguientes aspectos:

- El servicio de internet debe usarse exclusivamente para las actividades propias de la función desarrollada en la empresa y no debe utilizarse para ningún otro fin, teniendo en cuenta la política: Uso aceptable de los activos.
- Los usuarios autorizados para acceder al servicio de internet en **ALCALDÍA DE CAJICÁ** son los responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de la empresa.
- El oficial de seguridad es responsable de monitorear el tráfico y las comunicaciones establecidas en el servicio de internet **ALCALDÍA DE CAJICÁ**, para evitar las vulnerabilidades que puedan afectar la información de la empresa.

- Por ningún motivo el servicio de internet puede ser usado para descarga de información masiva de gran tamaño que pueda llegar a colapsar la red.
- Por ningún motivo el servicio de internet debe ser usado para descargar o visualizar información y contenidos que puedan atentar contra la seguridad de la información de **ALCALDÍA DE CAJICÁ** según lo contemplado en la política Controles contra códigos maliciosos.
- El Oficial de Seguridad de la Información debe monitorear el nivel de seguridad en los servicios de red que soporta el servicio de internet, teniendo en cuenta la política Seguridad de los servicios de red.
- Los usuarios no deben acceder a páginas relacionadas con pornografía, anonimizadores, actividades criminales y/o terrorismo, crímenes computacionales, hacking,

discriminación, contenido malicioso, suplantación de identidad de empresa, pornografía, spyware, adware, redes peer to peer (p2p), juegos, apuestas online, entre otras, que puedan afectar la seguridad de la información.

- Acceder a Internet por el canal contratado y aprobado por la empresa. No se autoriza acceder a internet desde los dispositivos de la empresa a través de canales diferentes a los autorizados.
- No se permite la descarga, uso, intercambio y/o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, entre otros.
- Informar, en caso de recibir información en archivos adjuntos de dudosa procedencia, al Oficial de Seguridad, quién escalará el incidente de seguridad a quién corresponda al interior de la empresa, para analizar y evitar la

materialización de cualquier tipo de riesgo que pueda afectar algún activo de información.

- Las conexiones directas de salida a internet no están permitidas, sin pasar por un firewall o un proxy.
- No se permite la conexión de dispositivos de comunicaciones como puntos de acceso inalámbricos o switches externos o internos, que no estén autorizados por el Oficial de Seguridad de la Información.

3.19. Seguridad Física - Dispositivos de Seguridad Contra *Incidencias*

Políticas Relacionadas: Inventario de activos, Política de control y Administración de accesos, Perímetro de seguridad física, Controles de accesos Físicos, Ubicación y protección de los equipos, Seguimiento y revisión de los servicios de los proveedores.

Objetivo: Definir el tipo y características de los dispositivos de seguridad contra incidencias que se presenten en el Centro de Datos donde se encuentran almacenados los servidores y equipos de misión crítica **ALCALDÍA DE CAJICÁ**, bien sea que el Centro de Datos sea propio o contratado.

Alcance: Esta norma define las condiciones a nivel de dispositivos de protección que se deben tener en el Centro de Datos, bien sea que este sea propio o contratado.

Descripción: En el Centro de Datos deben existir dispositivos de seguridad que garacen la detección temprana de incidencias consideradas como mínimas a controlar.

Para tal efecto se debe tener en cuenta los siguientes aspectos:

- **ALCALDÍA DE CAJICÁ** sigue siendo responsable del impacto que puedan provocar los incidentes en los Centros de datos a cargo de terceros, según la política 015 Seguimiento y revisión de los servicios de los proveedores.

- Debe existir un sistema de detección y prevención de incendios en el Centro de datos, que minimice el impacto que pueda generar la ocurrencia de un evento o situación de incendio en el lugar. Así mismo, se debe contar con un sistema de control de acceso que permita registrar el ingreso del personal.
- Debe existir un sistema de refrigeración en el centro de datos que sea capaz de generar alarmas en caso de mal funcionamiento y de esta forma permitir que se tomen medidas preventivas antes de que se pueda materializar un riesgo por daño de equipos.
- Debe existir un sistema de regulación y estabilización del fluido eléctrico, el cual debe generar y notificar alarmas y eventos relacionados con la energía, y de esta forma permitir que se tomen medidas preventivas antes de que se pueda

materializar un riesgo de daño de equipos.

3.20. Seguridad Física –Backups

Políticas Relacionadas: Inventario de activos, Política de control y Administración de accesos, Respaldo de la información. Perímetro de seguridad física, Controles de accesos Físicos, Seguridad de las oficinas, recintos e instalaciones, Ubicación y protección de los equipos,

Objetivo: Definir los controles de acceso físico que deben existir en los lugares donde se resguarden los backups **ALCALDÍA DE CAJICÁ**.

Alcance: Esta norma define los controles de seguridad física instalados en los lugares donde se guardan dispositivos que almacenan los backups **ALCALDÍA DE CAJICÁ**.

Descripción: Adicionalmente a las medidas de control de acceso y dispositivos de control de incidencias ya descritas en las normas de seguridad física respectiva, debe tenerse en cuenta los siguientes aspectos:

- Los respaldos deben ser almacenados en un sitio suficientemente seguro de **ALCALDÍA DE CAJICÁ** que les permita mantener su integridad ante la ocurrencia de un desastre en las instalaciones. En los casos de activos críticos, el Oficial de Seguridad de la Información determinará si los respaldos de la información deben ser almacenados en un sitio externo a **ALCALDÍA DE CAJICÁ**.
- Todos los cambios estructurales a ejecutarse los lugares destinados al almacenamiento de copias de respaldo, deben ser consultados con el Oficial de Seguridad a fin de que se evalúe antes de la realización de los mismos, las posibles consecuencias sobre la seguridad física.

3.21. Gestión de Incidentes de Seguridad de la Información Responsabilidades y procedimientos

Políticas Relacionadas: Responsabilidades y procedimientos (Gestión de incidentes de seguridad de la información), Reporte de eventos de seguridad de la información, Evaluación de eventos de seguridad de la información y decisiones sobre ellos, Aprendizaje obtenido de los incidentes de seguridad de la información, Recolección de evidencia.

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Alcance: Esta norma define las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información

Descripción: La Gestión de Incidentes de seguridad de la información se llevará a cabo de acuerdo al documento Procedimiento de Gestión de Incidentes de Seguridad, según las siguientes etapas:

- Detección o reporte del incidente: Los colaboradores de cada área son los encargados de reportar al Oficial de Seguridad de la Información sobre los incidentes presentados en su área, con el fin de gestionarlos, mitigando así el impacto que los incidentes generan. La oficina TIC puede considerar implementar un sistema de gestión de incidentes automatizado que facilite al usuario el reporte de los incidentes.

Adicionalmente, el Oficial de Seguridad de la Información, con apoyo del jefe de la Oficina TIC, debe definir y liderar la implementación de los mecanismos adecuados para la detección de incidentes de seguridad asociados a cualquiera de los estados de la información: En uso (por parte del usuario final o por parte de un proceso en un servidor), en movimiento (en tránsito en la red LAN o WAN) o en reposo (cuando está almacenada).

Igualmente se deben revisar los informes o reportes periódicos de eventos sucedidos a los servidores, aplicativos y equipos de comunicaciones a fin de detectar posibles anomalías y en caso de que aplique, reportar un incidente de seguridad de la información.

- Análisis del incidente reportado: El Oficial de Seguridad de la Información debe clasificar el tipo de incidente y establecer su prioridad de acuerdo al Procedimiento de Gestión de Incidentes. Esto con el objetivo de dar prioridad a aquellos incidentes que se cataloguen como críticos dentro de la empresa. Igualmente se debe identificar si el incidente ocasionó el incumplimiento a alguna normatividad aplicable, incluidas la Ley 1273 de 2009 o la Ley 734 de 2002 - Código Disciplinario Único.

- Recolección de evidencia: El Oficial de Seguridad de la Información debe liderar el proceso de recolección de evidencia forense del incidente en caso de que se requiera con el fin de

utilizar dicha información como prueba si se hace una acusación formal contra el atacante o sus cómplices.

- Contención o preparación de la solución del incidente: Acorde con la prioridad en la que se clasifique el incidente se deben establecer medidas de mitigación

Calle 2 No. 4-07 - Cajicá - Cundinamarca - Colombia
Código postal: 250240 PBX (57+1) 8795356 - 8837077
Correo: contactenos-pqrs@cajica.gov.co Página web: www.cajica.gov.co
icontec ISO 9001
CO-SC-CER-701118
CERTIFIED IQNet MANAGEMENT SYSTEM

inmediatas con el fin de gestionar el mismo. Estas son medidas de choque para evitar aumentar el impacto, hasta el momento en que se realice una acción definitiva para solucionar el incidente de forma definitiva.

- Solución del incidente: Para dar una solución eficaz al incidente se debe evaluar y analizar la información de incidentes similares que se hayan presentado en la empresa consultando la base de datos del conocimiento. A continuación, el Oficial de Seguridad de la Información debe definir la solución más adecuada para el incidente y planear un conjunto de actividades a realizar con sus respectivos responsables con el fin de solucionar el incidente.

- Recuperación y seguimiento del incidente: Se debe hacer seguimiento a las actividades implementadas para erradicar el incidente de seguridad y se deben evaluar los resultados de forma conjunta entre el colaborador que reporta el incidente y el Oficial de Seguridad de la Información. Si se considera que las actividades realizadas gestionaron adecuadamente el incidente se procederá a su cierre, si por el contrario no se gestionó de forma adecuada se vuelve a plantear una nueva solución.

- Registro y comunicación del incidente: El Oficial de Seguridad de la Información debe llevar un registro documental del incidente de seguridad con el fin de garantizar la trazabilidad sobre los mismos al igual que para permitir aprender de ellos y utilizar la información histórica para la toma de decisiones en incidentes futuros. Adicionalmente el Oficial de Seguridad de la Información debe solicitar un informe que describa la forma como se atendió y solucionó en incidente de seguridad.

3.22. Reporte de eventos de seguridad de la información.

Políticas Relacionadas: Responsabilidades y procedimientos (Gestión de incidentes de seguridad de la información), 045 Reporte de eventos de seguridad de la información, Evaluación de eventos de seguridad de la información y decisiones sobre ellos, Aprendizaje obtenido de los incidentes de seguridad de la información, Recolección de evidencia.

Objetivo: Definir los canales de gestión para el reporte rápido y oportuno de los eventos de Seguridad de la Información.

Alcance: Esta norma define los canales de gestión apropiados para el reporte de eventos de Seguridad de la Información.

Descripción:

- Todos los colaboradores de **ALCALDÍA DE CAJICÁ** y terceros deben reportar al Oficial de Seguridad de la Información cualquier evento o debilidad de

seguridad que pueda afectar la confidencialidad, integridad o disponibilidad de la información.

- Los canales autorizados para el reporte de eventos o debilidades de seguridad de la información son los siguientes: 1) Vía correo electrónico: soluciones@gophergroup.com.co, 2) Vía llama telefónica: PBX 7039170 ext.108.

- El Oficial de Seguridad de la Información con el apoyo del área que realice las funciones de comunicación organizacional dentro de **ALCALDÍA DE CAJICÁ**, debe realizar el proceso de divulgación de Plan de Continuidad de Negocio a todos los colaboradores **ALCALDÍA DE CAJICÁ**.

3.23. Disponibilidad de instalaciones de procesamiento de información

Políticas Relacionadas: Disponibilidad de las instalaciones de procesamiento de información.

Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de información de **ALCALDÍA DE CAJICÁ** con el fin de cumplir los requisitos de disponibilidad de la Empresa.

Alcance: Esta norma define los controles necesarios a nivel de infraestructura tecnológica para satisfacer los requisitos de disponibilidad **ALCALDÍA DE CAJICÁ**.

Descripción:

- Las instalaciones de procesamiento de información (principales o alternas) deben estar en condiciones físicas y ambientales propicias para garantizar la correcta ejecución y restablecimiento de las operaciones cuando sea necesario. Esto impacta directamente la integridad y disponibilidad de la información **ALCALDÍA DE CAJICÁ**.
- En caso de que se tenga tercerizado el uso de infraestructura, plataforma hardware, software remoto (por ejemplo en un centro de datos principal/ alterno o a través de una solución de computación en la nube), el supervisor de dicho contrato debe validar la existencia de acuerdos de nivel de servicios (ANS) que definan de forma clara las condiciones del servicio, que incluyen: disponibilidad porcentual, MTBF (Mean Time Between Failure), efectividad en la instalación, efectividad en la ampliación de capacidades (elasticidad y flexibilidad), efectividad en la atención de solicitudes, calidad de los reportes entregados, servicios de operación y administración, gestión de seguridad, etc.
- Los acuerdos de nivel de servicio (ANS) establecidos deben ser monitoreados y revisados regularmente en la etapa contractual para garantizar que se cumple con lo contratado y que se logran los objetivos de disponibilidad **ALCALDÍA DE CAJICÁ**.

Se debe considerar lo definido en los Acuerdos Marco Vigentes definidos por Colombia Compra Eficiente, especialmente aquellos asociados a Servicios de nube pública y Servicios de centro de datos / nube privada, esto teniendo en cuenta los diferentes esquemas del modelo de computación en la nube: Software como servicio (SaaS), Plataforma como servicio (PaaS), Infraestructura como servicio (IaaS).

- El Oficial de Seguridad de la Información debe establecer los esquemas de cifrado necesarios para garantizar la confidencialidad en la sincronización/replicación de la información desde el centro de datos principal hacia el centro de datos de respaldo (en caso de que exista uno). Para esto se deben considerar diferentes esquemas de cifrado:

- Cifrado individual de archivos o carpetas
- Cifrado a nivel del sistema de archivos (por ejemplo mediante un sistema EFS)
- Cifrado de una porción de la información (por ejemplo en el caso de aplicaciones mediante un cifrado a nivel de base de datos)
- Cifrado en todo el canal de transmisión (por ejemplo mediante una VPN)
- Cifrado de la conexión hacia ciertas aplicaciones (por ejemplo mediante conexiones https)

- El Oficial de Seguridad de la Información debe liderar el monitoreo regular de la replicación de la información de **ALCALDÍA DE CAJICÁ** hacia el centro de datos contratado, para ello se deben llevar registros de las labores de sincronización y en caso de errores relacionados a la integridad, confidencialidad o disponibilidad de los datos, evaluar la generación de un incidente de seguridad de la información, mediante el procedimiento de gestión de incidentes.
- Los backups realizados sobre la información almacenada en el centro de datos principal/alterno o en una arquitectura de computación en la nube deben estar sujetos a la política 020 Respaldo de la Información. Esto implica seguir los lineamientos en cuanto a pruebas sobre los backups realizados y validación de su restauración.

3.24. Gestión de la Prestación de Servicios de Proveedores. Política de Gestión de Proveedores

Políticas Relacionadas: Seguimiento y revisión de los servicios de los proveedores.

Objetivo: Definir los mecanismos para realizar un monitoreo y auditoria a los servicios, reportes y registros provistos por los proveedores.

Alcance: Esta norma cubre a los proveedores y terceros que colaboran con la empresa.

Descripción:

- El proceso de gestión de servicios por parte de **ALCALDÍA DE CAJICÁ** a los proveedores y terceros se debe llevar a cabo bajo los siguientes lineamientos a cargo del Oficial de Seguridad con la colaboración del Coordinador de Servicios Tecnológicos y el Responsable de Gestión de Proyectos de Sistemas de Información:

- Se debe monitorear los Acuerdos de Niveles de Servicio (ANS) concertados con cada proveedor o tercero para validar su cumplimiento y tomar medidas correctivas a que haya lugar.

- Se deben revisar los reportes de servicio entregados por los proveedores o terceros para verificar el cumplimiento de las actividades desarrolladas y de ser necesario programar reuniones de seguimiento.

- Se debe suministrar la información y elementos necesarios al proveedor o tercero cuando este es requerido para atender un incidente de seguridad conforme esté estipulado en los lineamientos del soporte y los ANSs.

- Se deben hacer seguimientos de auditoria a contratistas y terceros teniendo en cuenta los registros de eventos de seguridad, problemas operacionales, interrupciones de servicio, y demás incidentes relacionados con la manipulación de los contratistas o terceros.

- Se debe dar solución a cualquier incidente detectado en el cual estén involucrados los proveedores o terceros.

- Se deben tomar las acciones correspondientes conforme a las cláusulas de los contratos y los ANSs.

- **ALCALDÍA DE CAJICÁ** en cabeza del Oficial de Seguridad debe siempre mantener el control de todos los sistemas de seguridad de la información que pueden verse afectados por la información confidencial o crítica que las personas contratistas o terceros ingresan, procesan o manejan.
- El Oficial de Seguridad debe establecer una estructura de reportes, formato o proceso que permita hacer trazabilidad o seguimiento a las actividades desarrolladas por los contratistas o terceros.

- Las actividades programadas para ser ejecutadas por un contratista o tercero deben ser validadas por el Oficial de Seguridad con el apoyo del funcionario responsable directo de dicha actividad y someterse al proceso de control de cambios para su aprobación final.

3.25. Cumplimiento de los requisitos legales. Protección de datos personales

Políticas Relacionadas: Privacidad y protección de información de datos personales
Objetivo: Garantizar la privacidad y la protección de los datos personales de todas las personas que interactúen con **ALCALDÍA DE CAJICÁ**, para tal fin, se establecerán instrumentos y controles para el adecuado tratamiento de los datos.

Alcance: **ALCALDÍA DE CAJICÁ** en su calidad de responsable del tratamiento de datos personales, define su alcance para la norma Protección de datos personales teniendo en cuenta la Ley 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales",

Descripción:

- Es responsabilidad de la Superintendencia del Subsidio Familiar en cumplimiento de su deber legal y reglamentario, hacer efectiva la garantía constitucional de protección a la intimidad personal y familiar de todos los ciudadanos, estableciendo instrumentos y controles de cara a dar un tratamiento adecuado a la información que administra.

- La empresa asegura la debida reserva de la información personal de las personas o empresas que se encuentran en su base de datos, la cual será utilizada para el envío de información institucional de la empresa.

- La empresa no proporciona la información de sus grupos de interés a ningún tercero, salvo que la persona o empresa lo autorice de forma expresa y por escrito.

- La información obtenida en cualquier registro de datos personales realizado en forma presencial y/o virtual para algún producto o servicio **ALCALDÍA DE CAJICÁ**, será utilizada solo para fines institucionales, en ningún momento será compartida ni transferida a terceros para su utilización.

- Las empresas o personas pueden decidir, conocer, actualizar, rectificar y solicitar la eliminación de sus datos personales en cualquier momento a la empresa.

- Para los casos en donde no se puede determinar la voluntad de las personas que comparten sus datos personales con **ALCALDÍA DE CAJICÁ**, la empresa debe implementar mecanismos de ocultación u ofuscación de datos sensibles en sus sistemas para evitar la violación de la legislación.

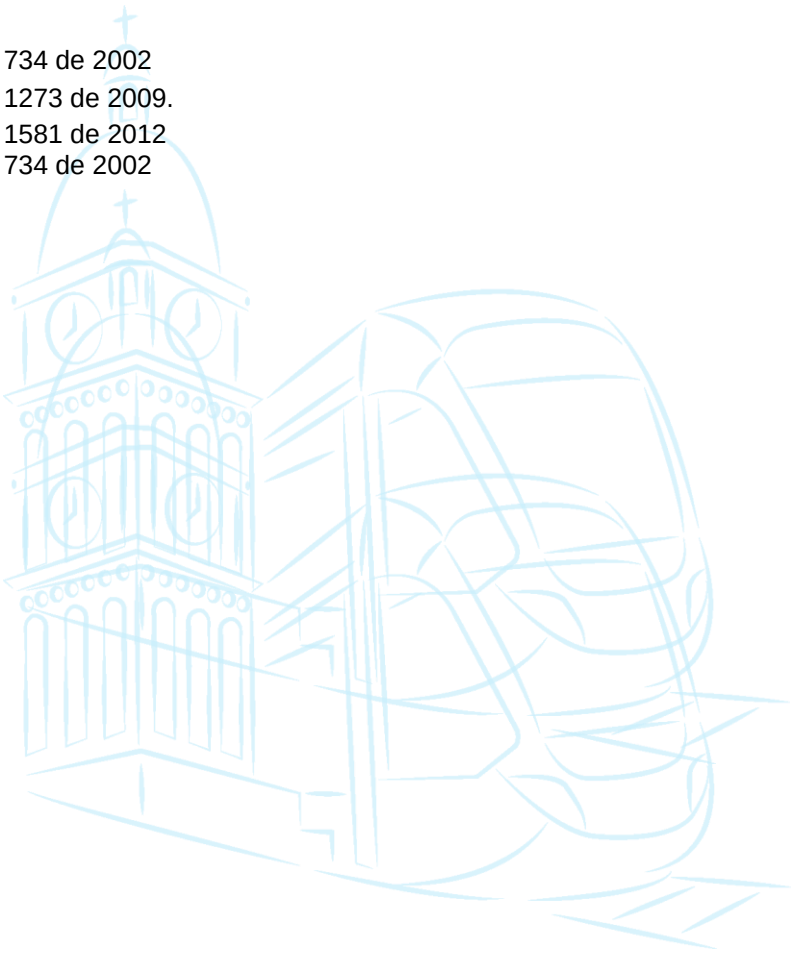
- Todos los contratistas y terceros dentro de **ALCALDÍA DE CAJICÁ** deben cumplir la cláusula de confidencialidad de la información y la cláusula de integridad de la información, definidas en sus contratos. Por otra parte a los funcionarios les aplica el código disciplinario único de la Ley 734 de 2002, en

particular el artículo 34 (deberes de todo servidor público) y 48 (faltas gravísimas).

REFERENCIAS BIBLIOGRÁFICAS

Ley 734 de 2002

Ley 1273 de 2009.

Ley 1581 de 2012

Ley 734 de 2002