Tabla de contenido

OBJETIVO GENERAL

El objetivo principal del Manual de Seguridad y Privacidad de la Información para la Alcaldía de Fusagasugá es establecer un conjunto de políticas, procedimientos y directrices que aseguren la protección de la información sensible y la privacidad de los datos manejados por la Alcaldía. Esto incluye la prevención de amenazas de seguridad, la garantía de la confidencialidad, integridad y disponibilidad de la información, y el cumplimiento marco legal y los lineamientos proporcionados por MinTIC

OBJETIVO ESPECÍFICOS

- Cumplir a conformidad con las normativas legales y regulaciones establecidas por la Alcaldía del municipio de Fusagasugá, en particular en lo que respeta a la seguridad de la información. Esto se enfoca específicamente en el cumplimiento de la estrategia de Gobierno Digital y las directrices del Modelo de Seguridad y Privacidad de la Información (MSPI) promovido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- Garantizar que el nivel de riesgo en cuanto a la Seguridad de la Información se mantenga en los niveles Bajo o Moderado, a través de la concientización en materia de seguridad de la información para el personal de la Alcaldía del municipio de Fusagasugá, en lo que respeta a la extensión y alcance del Modelo de Seguridad y Privacidad de la Información (MSPI).
- Ejecutar planes de tratamiento de forma inmediata y adecuada para abordar todos los escenarios de riesgo que superen el Nivel de Riesgo Aceptable (NRA) establecido por la Entidad.
- Registrar y llevar a cabo medidas, preventivas y correctivas frente a cualquier infracción de las Políticas de Seguridad de la Información, con el propósito de gestionar y resolver de manera oportuna los incidentes de seguridad de la información, a fin de reducir su impacto en los procedimientos de la Entidad.

1. ALCANCE

La cobertura para la implementación del Modelo de seguridad y privacidad de la información en la Alcaldía del municipio de Fusagasugá abarca todos los aspectos relacionados con la seguridad y la privacidad de la información. Es importante definir claramente el alcance para delimitar las áreas y actividades que están sujetas a las políticas y directrices establecidas en el manual.

El responsable de la aplicación y divulgación del presente manual, así como de los procedimientos y formatos del MSPI es el oficial de seguridad de la información o el funcionario designado para que haga sus veces.

2. RESPONSABLES

La seguridad de la información es una responsabilidad conjunta que involucra a todos (secretarios, director, jefe de oficina, funcionarios y contratistas), sin embargo el equipo de

seguridad de la información conformado por el Oficial de Seguridad de la Información y el comité de gestión y desempeño quienes juegan un papel importante en su gestión y supervisión.

3. DEFINICIONES

Acceso a la información pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
Activo de información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
Auditoria: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
Datos abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
Datos personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
Datos personales públicos: Es el dato que no sea semiprivado, privado o sensible. Son

considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos personales privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos personales mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos personales sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado de tratamiento de datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Ley de habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de trasparencia y acceso a la información pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Registro nacional de bases de datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Responsabilidad demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias

Responsable del tratamiento de datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Sistema de gestión de seguridad de la información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de datos personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Partes interesadas: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Copia de seguridad o copia 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.

Transferencia de información: Es el envío de información desde la entidad por parte de un funcionario, contratista o proceso automatizado hacia otra persona o proceso fuera de la organización.

Dispositivo móvil: También conocido como computadora de bolsillo o computadora de mano, es un tipo de computadora de tamaño pequeño, con capacidades de procesamiento, con conexión a Internet, con memoria, diseñado específicamente para una función específica.

Software: Es el soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados *hardware*.

Hardware: En informática se refiere a las partes físicas tangibles de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos. Cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado componen el hardware; contrariamente, el soporte lógico e intangible es el llamado *software*.

Sistemas de Información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. Dichos elementos formarán parte de alguna de las siguientes categorías: Personas, Actividades o técnicas de trabajo, Datos y Recursos materiales en general.

Aceptación del riesgo: La decisión informada para tomar un riesgo en particular.

Activo: Cualquier elemento que tiene valor para la organización y que para Gestión de riesgos de seguridad de la información se consideran los siguientes: información, software, elementos físicos, servicios, personas e intangibles.

Amenaza: Causa potencial de incidente no deseado, el cual puede resultar en daño al sistema o a la Organización.

Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento.

Causas: La razón por la cual se sucede el evento y cuya identificación depende del nivel de experiencia sobre el entorno y los elementos involucrados.

Certificado Digital: Archivo digital con los datos que se asocian a una Persona, Organismo o Entidad para suministrar identidad digital en las Redes de datos como Internet.

Confidencialidad: Propiedad de la información que hace que no sea revelada a individuos no autorizados, entidades o procesos.

Consecuencias: Resultado del evento que puede ser cierto o incierto y tener efectos positivos o negativos para la entidad y que puede expresarse en términos cualitativos o cuantitativos. Una consecuencia inicial puede tener mayor impacto considerando los efectos secundarios.

Criptoanálisis: Estudio de los sistemas criptográficos con el fin de encontrar debilidades en el sistema y romper su seguridad sin el conocimiento de las llaves correspondientes.

Disponibilidad: Propiedad de ser accesible y utilizable ante el requerimiento de una entidad autorizada.

Entidad Certificadora: Es un tercero de confianza encargado de emitir y revocar los certificados digitales.

Eventos: Presencia o cambio de un conjunto particular de circunstancias, que puede ser una o varias ocurrencias con una o varias causas. Un evento puede consistir en algo que no está sucediendo.
Fuentes de Riesgo: Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo. Una fuente de riesgo puede ser tangible como por ejemplo lo asociado con la tecnología o a las instalaciones y lo intangible como por ejemplo la situación sociocultural, entorno económico, clima político y entorno familiar.
Importancia del activo: Valor que refleja el nivel de protección requerido por un activo de información frente a las tres propiedades de la seguridad de la información: integridad, confidencialidad y disponibilidad.
Integridad: Propiedad de precisión y completitud.
Monitoreo: Verificación, supervisión, observación crítica o determinación del estado del activo con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

Parte involucrada: Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o una actividad. Una persona que toma decisiones puede ser una parte involucrada.
Propietario del activo: Persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.
Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización)
Riesgo residual: El riesgo que permanece tras la consideración de los controles existentes.
Vulnerabilidad: Debilidad identificada sobre un activo, que puede ser aprovechada por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información de la Alcaldía del municipio de Fusagasugá es una declaración que refleja la posición de la alta dirección en cuanto a la protección de los activos de información y la implementación del Modelo de Seguridad y Privacidad de la Información. Además, busca promover la divulgación y la mejora constante de estas prácticas.

La Alcaldía del municipio de Fusagasugá se compromete a gestionar la seguridad y la privacidad de la información a través de la incorporación, seguimiento y mejora continua de los controles necesarios. Estos controles están enfocados en una adecuada gestión de riesgos de seguridad de la información con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información bajo su responsabilidad. Esto se hace en cumplimiento de los marcos legales, normativos, regulatorios y contractuales aplicables a la entidad, fortaleciendo de esta manera la gestión e imagen institucional y los servicios que presta la

organización.

4.1. Directrices de la política de seguridad y privacidad de la información

Como complemento a la política general, de la Alcaldía del municipio de Fusagasugá se establecen las siguientes directrices:

- Es prioridad para la Alcaldía del municipio de Fusagasugá proteger la confidencialidad, integridad y disponibilidad de la información suministrada por los ciudadanos, funcionarios y proveedores del municipio que adelanten trámites relacionados con cualquiera de los procesos transversalmente cubiertos por el proceso de tecnologías de la información y las comunicaciones.
- Implementará los mecanismos suficientes para que los datos requeridos por los procedimientos relacionados con los procesos de inspección, control, vigilancia y gestión de recursos informáticos cumplan con los niveles de disponibilidad necesarios.
- El Oficial de Seguridad de la información, o quien haga sus veces, debe garantizar que los funcionarios de la Alcaldía del municipio de Fusagasugá dispongan de permanente actualización, entrenamiento y sensibilización sobre las políticas, procedimientos y demás documentos con base a los lineamientos de MINTIC para el MSPI.
- Los funcionarios de la Alcaldía del municipio de Fusagasugá son responsables de identificar y reportar los incidentes de seguridad de la información de los cuales sean víctimas o de los cuales tengan conocimiento.
- Todas las operaciones que se lleven a cabo sobre la información de la Alcaldía del municipio de Fusagasugá deben tener una previa validación para aplicar los controles requeridos frente a la confidencialidad, integridad y disponibilidad de los activos de información.
- Es mandatorio el cumplimiento de las Políticas, Procedimientos y demás documentos del MSPI en la medida que aplique para todos los funcionarios, contratistas, proveedores y demás partes interesadas de la Alcaldía del municipio de Fusagasugá.
- El compromiso del cumplimiento de los objetivos del MSPI está en cabeza del funcionario al que le sea asignado el rol de Oficial de Seguridad de la Información.

4.2. Principios de seguridad de la información

Los principios de seguridad de la información son fundamentos que guían la gestión y protección efectiva de los activos de información de la Alcaldía de Fusagasugá. Estos principios son clave para garantizar la confidencialidad, integridad y disponibilidad de la información. A continuación, se enumeran los principios de seguridad de la información:

Confidencialidad: Este principio asegura que la información solo esté disponible para aquellos que tienen la autorización para acceder a ella. Se logra a través de controles de

acceso, cifrado y clasificación de información.

Integridad: La integridad se refiere a la precisión y confiabilidad de la información. Los datos deben permanecer precisos y sin modificaciones no autorizadas a lo largo de su ciclo de vida. Esto se logra mediante la implementación de controles de integridad y sistemas de detección de modificaciones no autorizadas.

Disponibilidad: La información debe estar disponible y accesible cuando sea necesario. Esto implica garantizar que los sistemas estén en funcionamiento y se cuente con planos de continuidad de negocio y recuperación ante desastres.

Autenticación: La autenticación se refiere a la verificación de la identidad de un usuario o sistema que intenta acceder a la información. Esto se logra mediante contraseñas, tarjetas de acceso, biometría u otros métodos de autenticación.

Autorización: La autorización es el proceso de otorgar a los usuarios el acceso apropiado a la información y los recursos. Esto asegura que los usuarios solo tendrán acceso a la información que necesitan para llevar a cabo sus funciones.

No Repudio: El principio de no repudio se aplica a transacciones electrónicas y asegura que una vez que una parte ha realizado una acción, no puede negarla. Esto se logra mediante la implementación de mecanismos de registro y seguimiento.

Responsabilidad: La responsabilidad implica que los individuos y entidades sean responsables de sus acciones y actividades relacionadas con la información. Los registros de auditoría y la supervisión son esenciales para establecer la responsabilidad.

Sensibilización y Capacitación: La sensibilización y la capacitación de los empleados son cruciales para garantizar que estén al tanto de las políticas y prácticas de seguridad de la información y que puedan actuar de manera segura.

Evaluación y Gestión de Riesgos: La identificación y evaluación de riesgos son esenciales para determinar las amenazas a la seguridad de la información y tomar medidas para mitigar estos riesgos.

Cumplimiento Legal y Normativo: Cumplir con las leyes y regulaciones pertinentes, así como con estándares y normativas específicas, es fundamental para garantizar la legalidad y el cumplimiento en materia de seguridad de la información.

5. ADOPCIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y COMPROMISO DE LA ALTA DIRECCIÓN

El Modelo de seguridad y privacidad de la Información de la Alcaldía de Fusagasugá se adopta mediante Decreto, basado en lo establecido por la estrategia de Gobierno en Línea para las entidades territoriales y según el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la información y las Comunicaciones – MinTIC.

El Modelo de Seguridad y Privacidad de la Información se define como el conjunto de políticas, procedimientos y controles para proteger la confidencialidad, integridad y disponibilidad de la información de la Alcaldía del municipio de Fusagasugá, mitigando los riesgos al nivel bajo o moderado por la Alta Dirección. Los Despachos de las diferentes Secretarías, Jefes de Oficina y Coordinadores de Grupo de la Alcaldía del municipio de Fusagasugá manifiestan su compromiso con el Modelo de Seguridad y Privacidad de la

Información como un apoyo fundamental para el cumplimiento de sus objetivos y metas institucionales.

6. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

6.1. POLÍTICA DE CONTROL DE ACCESO

6.1.1. Objetivo de la política de control de acceso

La Política de Control de Acceso de la Alcaldía del municipio de Fusagasugá tiene como objetivo principal de esta política es garantizar que solo las personas autorizadas tengan acceso a la información y los sistemas, mientras se protege contra amenazas internas y externas.

6.1.2. Declaración general de la política de control de acceso

La Alcaldía de Fusagasugá reconoce la importancia crítica de la gestión adecuada del control de acceso a la información y los activos de la organización. La integridad, confidencialidad y disponibilidad de la información son fundamentales para el cumplimiento de nuestra misión de servicio público y la confianza de nuestros ciudadanos. Por lo tanto, la Alcaldía establece la siguiente política de control de acceso con el propósito de salvar la información y proteger los datos confidenciales.

6.1.3. Definición de privilegios de acceso

Los privilegios de acceso que se definan se deben basar en las funciones y responsabilidades del cargo o rol que desempeñe el funcionario, contratista o tercera parte que vaya a tener acceso a la información, siempre bajo el principio del mínimo privilegio posible de acuerdo con las necesidades de la Alcaldía del municipio de Fusagasugá.
Dichos privilegios deben estar definidos en lo referente a:

- Lectura
- Modificación
- Eliminación

De la misma manera, para las aplicaciones, se deben establecer los privilegios respecto a:

- Instalación
- Desinstalación
- Configuración
- Arranque de un servicio
- Detención de un servicio
- Funciones de auditoria

Para implementar esta definición por parte del dueño del proceso, se debe definir y mantener un esquema de roles y perfiles, con sus respectivos derechos y restricciones de

acceso a los diferentes sistemas de información, siguiendo el Procedimiento de Gestión de Cuentas de Usuario.

6.1.4. Condiciones de las cuentas de usuario

Las cuentas de usuario definidas para la Alcaldía del municipio de Fusagasugá deben cumplir estrictamente y sin ninguna excepción con las siguientes condiciones:

a. Cualquier cuenta de usuario a ser creada debe tener una justificación en una o más actividades que se encuentren formalmente definidas en uno o más procesos o procedimientos de la Alcaldía del municipio de Fusagasugá.
b. Todos los funcionarios y personal externo o subcontratado que accedan a los Sistemas de Información y recurso de las redes deberán registrarse y asociarse con un identificador personal e intransferible (un único nombre de usuario). La asignación de nombres o identificadores de usuario se debe realizar bajo el estándar definido por la Oficina de Tecnologías de la Información y las Comunicaciones para nombrar usuarios de la Alcaldía del municipio de Fusagasugá.
c. Todo sistema de información que tengan acceso a los sistemas principales de la entidad así este administrado por un proceso diferente a TI deben contar con identificadores asignados por la Oficina de Tecnologías de la Información y las Comunicaciones para nombrar usuarios de la Alcaldía del municipio de Fusagasugá.
d. No puede existir en un sistema una persona con más de una cuenta asignada pues no se podría asignar responsabilidad a una única persona.
e. Las cuentas de usuario son de uso personal e intransferible. Lo consignado en los registros (logs) de auditoría relacionadas con dichas cuentas, serán responsabilidad única del funcionario, contratista o tercera parte propietaria de la cuenta.
f. No puede haber una cuenta con acceso para más de una persona.
g. Los usuarios para cada sistema deben poseer una única cuenta de usuario.
h. En ningún caso se puede aceptar la suplantación o uso de una cuenta por parte de una persona diferente a la que le fue asignada. Toda persona que disponga de cuentas de acceso será responsable de mantener su confidencialidad y asegurar su correcto uso.
i. Se deben implementar mecanismos en los sistemas de la Alcaldía del municipio de Fusagasugá que permitan mantener la fortaleza de las contraseñas. Estos mecanismos son, entre otros:

- ✓ Cambio obligatorio de la contraseña después del primer ingreso.
- ✓ Cambio periódico de la contraseña.
- ✓ Bloqueo de la cuenta por un determinado número de intentos de autenticación fallidos.
- ✓ Validación de complejidad de la contraseña o Historial de acceso.

6.1.5. Gestión de cuentas de usuario

La gestión de cuentas de usuario en la Alcaldía del municipio de Fusagasugá debe seguir el Procedimiento de Registro y Cancelación de Cuentas de Usuario. Adicionalmente se

deben seguir los siguientes lineamientos:

El secretario de despacho, Jefe de Oficina, Director, dueños de proceso y supervisores de contrato deben reportar al Proceso de Gestión Humana de forma inmediata, las novedades de retiro temporal o permanente de funcionarios y contratistas a su cargo; el Proceso de Gestión Humana por su parte debe realizar en el menor tiempo posible las validaciones pertinentes para autorizar la novedad y la respectiva eliminación o bloqueo de las cuentas de usuario, correo electrónico y demás, efectuando la gestión y verificación pertinente con el proceso o persona a la que le corresponde eliminar, boquear o inactivar la cuenta e informar oportunamente la novedad al Oficial de Seguridad de la Información, o quien haga sus veces.

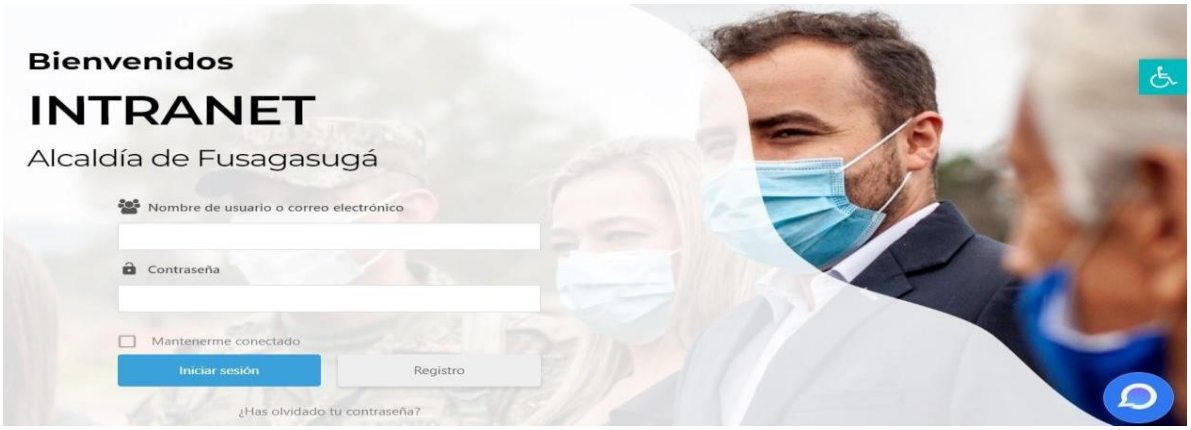
a. El cambio de cargo o rol en un funcionario debe seguir los pasos correspondientes de eliminación y posterior adición de la nueva cuenta que representa al funcionario.
b. No serán admitidas las modificaciones sobre los privilegios de acceso de una cuenta existente. La única forma permitida para los cambios de privilegios de acceso es mediante el cambio de un rol. Si se evidencia que para un rol determinado es necesario cambiar sus privilegios de acceso esto se debe formalizar siguiendo el Procedimiento de Gestión de cuentas de usuario.
c. El secretario de despacho, Jefe de Oficina, Director, dueños de proceso y supervisores de contrato deben revisar al menos una vez cada tres meses los privilegios de acceso asignados a su información, y debe reportar de manera inmediata como un evento de seguridad cualquier irregularidad, como podría ser por ejemplo un usuario todavía asignado y activo a un funcionario que ya no trabaja en esa área.
d. Los funcionarios de la Oficina de Tecnologías de la Información y las Comunicaciones actúan únicamente como custodios de la información y no pueden tomar decisiones sobre el acceso a la información que no sea de su propiedad.
e. Cuando un usuario olvide su contraseña de inicio de sesión, en ningún caso la Mesa de Ayuda o el Administrador de la plataforma podrán restablecerla sin validar que el usuario que se comunica a reportar el olvido sea quien afirma ser, y sin verificar con el encargado de área dueña de la información que sea un usuario con los privilegios de acceso aún vigentes.
f. La Oficina de Tecnologías de la Información y las Comunicaciones establecerá mecanismos automatizados de registro, monitorización de acceso y uso de los sistemas.
g. Las contraseñas predefinidas que traen los elementos nuevos tales como servidores, bases de datos, aplicaciones, routers, switches, y demás elementos activos de red, se deberán cambiar inmediatamente al poner en servicio el equipo; las cuentas de administrador de estos equipos deben cumplir también con todo lo definido en la presente política.

6.1.6. Control de acceso a redes y servicios de RED

Para el control de acceso a las redes y servicios de red de la Alcaldía del municipio de

Fusagasugá se deben seguir los siguientes lineamientos:

Para evitar duplicidad de políticas, procedimientos y formatos luego de ser revisada la documentación existente se deben seguir las instrucciones y demás lineamientos señalados en los documentos aprobados para el proceso GESTIÓN TIC, Acceso por el sitio web: https://intranet.alcaldiafusagasuga.gov.co/



En resumen, la visión de la política es:

a. Los funcionarios o terceras partes que necesiten conectarse para el desarrollo de sus funciones a la Red corporativa y/o WIFI de la Alcandía del municipio de Fusagasugá deben ser autorizados por el dueño del proceso para el cual desempeñan sus funciones, actividades u obligaciones, y deben conocer, acoger y dar cumplimiento a las políticas, procedimientos y demás lineamientos de Seguridad de la Información de la Alcaldía de Fusagasugá, incluyendo las directrices distribuidas por el Directorio Activo para usuarios finales; además dentro de sus responsabilidades están:

- Identificar las debilidades de seguridad y posibles riesgos de seguridad de la información sobre los activos a los cuales tengan acceso o conocimiento e informar a los dueños de la Información y al Oficial de Seguridad de la Información o quien haga sus veces.
- Brindar información y participar en las actividades de investigación de incidentes de seguridad de información, de acuerdo a como se le requiera.
- Participar en el proceso de capacitación, sensibilización y aprobación de Seguridad y Privacidad de la Información de la Alcaldía de Fusagasugá, para implementar la cultura organizacional en este tema.
- Generar sugerencias para mejorar la Seguridad de la Información de la entidad.
- Reportar de manera oportuna los eventos o incidentes que afecten la seguridad y privacidad de la información.

b. Los equipos propiedad de la Alcaldía del municipio de Fusagasugá solo podrán

conectarse a otras redes, incluyendo Internet, a través de la Red corporativa de la Alcaldía del municipio de Fusagasugá. Está prohibido que los equipos propiedad de la Alcaldía del municipio de Fusagasugá se conecten a través de módems, celulares o cualquier otro dispositivo que le permita acceder directamente a Internet o cualquier otra Red.

c. Los accesos originados desde otra Red a un equipo dentro de la Red de la Alcaldía del municipio de Fusagasugá deben realizarse siempre a través de una VPN.

d. El acceso para tomar control remoto de un equipo no deberá darse sin la autenticación del mismo y sin la autorización del usuario responsable del mismo, y siempre debe contar con su aprobación.

e. No se recomienda el uso de equipos personales para que los funcionarios y contratistas desempeñen actividades relacionadas con su trabajo en el Alcaldía del municipio de Fusagasugá. En todo caso, es el director, subdirector, jefe o coordinador del área donde se usaría el equipo personal quien debe autorizar su uso y tramitar la conexión del mismo a la Red de la Alcaldía del municipio de Fusagasugá.

f. La Oficina de Tecnologías de la Información y las Comunicaciones deberá configurar y monitorear que todas las conexiones entre las redes de la Alcaldía del municipio de Fusagasugá y redes externas pasen a través de un sistema de firewall que controle las direcciones de origen y destino. También será responsable de verificar que sólo los protocolos autorizados poseen permisos para cruzar la frontera de la Red de la Alcaldía del municipio de Fusagasugá.

g. Todo funcionario o contratista que acceda al correo electrónico institucional desde una plataforma diferente a la que proporciona el Alcaldía del municipio de Fusagasugá (por ejemplo, tabletas, celulares, portátiles personales, etc.) son los responsables por su buen uso.

6.1.7. Control de acceso físico

Cada director, subdirector, jefe de oficina o coordinador de grupo debe definir si es necesario proteger la información física o los equipos de su dependencia mediante el establecimiento de perímetros de seguridad física, de acuerdo con la clasificación de la información y a los riesgos de seguridad identificados sobre la misma. El Oficial de seguridad de la información, o quien haga sus veces, debe posteriormente tramitar con el área de seguridad física la protección de dichas áreas, a las cuales se les denominará denomina áreas seguras o zonas restringidas.

- La alcaldía de Fusagasugá deberá contar con los mecanismos de vigilancia de acceso tales como sistemas de control (identificación usuarios) y sistema de comunicación de los guardas a cada una de las dependencias que la institución considere necesario
- al ingresar todos los usuarios a la entidad se realiza un registro en la ventanilla, solicitando datos personales completos, como nombres y apellidos, número de

documento de identidad, correo electrónico, numero de celular, se le preguntara para que dependencia se dirige y si está agendado, se verifica que elementos ingresa en caso que sea un computador, se deben colocar todas las características, como modelo y marca. una vez terminado este proceso se le activa la huella para que pueda pasar por la talanquera.

- La talanquera contara con acceso de personas en condición de discapacidad el cual está diseñado para todos aquellos usuarios tengan alguna dificultad a la hora de su entrada y salida de la entidad.
- Los usuarios de los servicios prestados por las oficinas de la institución deben ser guiados por un empleado autorizado, asesor o contratista. esto significa que se requiere de señalización para llegar a las oficinas sin perdida ya que es lo que más se presenta en la entidad debido a que los guardas dan una indicación muy superficial porque no pueden retirarse de su puesto de vigilancia.
- Tan pronto como un usuario entra a un área y hasta que este salga se deberá tener control por parte de los guardas que no entre a lugares no autorizados.
- Siempre que un funcionario note que un usuario se encuentra dentro de áreas restringidas de la institución, el usuario debe ser inmediatamente cuestionado acerca de su propósito de encontrarse en esta área e informar a los responsables de la seguridad del edificio.
- Para el acceso a los espacios de archivo tanto en las dependencias como en el archivo central, se debe dar aplicación a los controles establecidos en la entidad y todo debidamente documentado.
- Control de acceso con usuario y contraseña debidamente segura que cumpla con requerimientos establecidos por parte del funcionario a cargo de esta, se debe elaborar un proceso sobre control de acceso a redes, aplicaciones, y/o sistemas de información de la entidad.
- El Centro de Comunicaciones (Datas) y las áreas que la institución considere, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares (oficina tic).
- Instalar talanquera en todas las sedes de la alcaldía y manejar el mismo control en el momento del ingreso para mejor control de acceso de los usuarios.

6.2. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

6.2.1. Objetivo de la política

La Política de Escritorio y Pantalla Limpia de la Alcaldía del municipio de Fusagasugá busca asegurar que sus funcionarios y contratistas adopten mejores prácticas de seguridad de la información en cuanto al uso de los espacios de trabajo y las herramientas y provistas por la entidad.

6.2.2. Declaración general de la política de escritorio y pantalla limpia

Todos los funcionarios de la Alcaldía del municipio de Fusagasugá y terceros a los que se dé acceso a información son responsables por la debida diligencia para prevenir el acceso no autorizado a la pantalla de su equipo y a la información impresa que esté a su cargo.

Considerando los requerimientos para la Confidencialidad, Integridad y Disponibilidad de los activos de información que cada funcionario, contratista y personal tercerizado maneja se ha definido una línea base para ser aplicada en forma general a todo la Alcaldía del municipio de Fusagasugá en cuanto a la disposición del escritorio y el acceso visual a la pantalla de cada equipo de cómputo.

6.2.3. Escritorio

Los activos de información deben recibir un tratamiento basado en la clasificación recibida aplicando lo definido en la política de uso aceptable de los activos de la Alcaldía del municipio de Fusagasugá.

En el caso de los activos de información que son documentos impresos, su protección debe aplicarse para que estos no se encuentren sin custodia o restricción de acceso en algún momento, por esto cada funcionario, contratista o personal tercerizado de la Alcaldía del municipio de Fusagasugá debe aplicar las siguientes reglas sobre el uso de su escritorio de Trabajo:

a. Los documentos impresos que correspondan a activos de información catalogados como Públicos Clasificados o Públicos Reservados que estén siendo utilizados no pueden encontrarse encima del escritorio, salvo que estén siendo consultados en eseinstante por el funcionario, contratista o personal tercerizado autorizado.
b. En ausencia del funcionario, contratista o personal tercerizado responsable, el escritorio debe permanecer despejado sin ningún tipo de documento impreso y la información deberá ser almacenada bajo llave.
c. Se debe mantener en estricto orden y limpieza el puesto de trabajo.
d. Se recomiendan todas las medidas preventivas al momento de consumir bebidas y alimentos en el puesto de trabajo, considerando que el verter líquidos puede causar daños en los documentos y/o equipos electrónicos y esto será responsabilidad del funcionario, contratista o personal tercerizado.
e. Todo documento que no esté siendo utilizado y que sea clasificado como Público Clasificado o Público Reservado, debe estar salvaguardado bajo llave en un archivador destinado para ese fin.
f. Toda información considerada como Pública Clasificada o Pública Reservada escrita sobre tableros o paredes de oficinas o salas de juntas, deberá ser eliminada una vez finalice una reunión.

6.2.4. Cierre de sesión

Todo funcionario, contratista o personal tercerizado debe bloquear la sesión en su equipo al levantarse de su puesto de trabajo, y adicionalmente debe tener habilitado el bloqueo

automático de sesión por inactividad, de tal manera que la sesión se encuentre siempre cerrada cuando el puesto se encuentre sin custodia. Para habilitar nuevamente la sesión se deberá digitar nuevamente el usuario y contraseña.

Si está habilitado el protector de pantalla, este será provisto por la Alcaldía del municipio de Fusagasugá y no se admite el uso de software o un diseño diferente al establecido.

6.2.5. Medidas de supervisión

El personal de vigilancia podrá realizar rondas al medio día y al finalizar la jornada laboral para ejecutar el siguiente procedimiento:

- Recoger y salvaguardar los documentos que se encuentren encima del escritorio de los funcionarios, contratistas o personal tercerizado.
- Recoger y salvaguardar los dispositivos que se encuentren sin custodia.
- En caso de encontrar equipos sin custodia y con la sesión abierta, deberá bloquear la sesión y dejar el registro de la situación.

- Cuando cualquier funcionario identifique en cualquier momento alguno de los hechos descritos anteriormente, debe proceder a reportarlo como un incidente de seguridad.

6.2.6. Sanciones por incumplimiento

En los primeros seis meses se establecerá un periodo pedagógico después del cual se procederá con el esquema de sanciones acorde con lo establecido por la Oficina de Control Interno Disciplinario.

6.3. POLÍTICA DE USO ACEPTABLE DE LOS ACTIVOS

6.3.1. Objetivo de la política

La Política para el Uso Aceptable de los Activos de la Alcaldía del municipio de Fusagasugá busca que cada funcionario o contratista sepa cuál es el tratamiento que debe tener para cada uno de los activos asociados a la información que esta tenga a su cargo en lo referente a seguridad de la información.

6.3.2. Declaración general de la política de uso aceptable de los activos

La Alcaldía del municipio de Fusagasugá establece que cada activo de información debe tener definido un uso aceptable que establece las acciones permitidas y las restricciones que deben ser aplicadas por quienes hagan uso del mismo. Esta definición es responsabilidad exclusiva del propietario del activo.

6.3.3. Uso de los activos

a. Los activos de información que pertenecen a la Alcaldía del municipio de Fusagasugá deben utilizarse exclusivamente con propósitos laborales, de forma ética y en cumplimiento de las leyes y reglamentos vigentes.
b. Es responsabilidad del funcionario o contratista el cuidado, manejo y cumplimiento de los requisitos de seguridad de la información en los activos de información que le sean asignados o que estén a su cargo.
c. La instalación de software en los equipos de cómputo suministrados por la Alcaldía del municipio de Fusagasugá y de los equipos conectados a la Red corporativa es una función exclusiva de TI, y por tanto toda solicitud de instalación debe tramitarse a través de una solicitud al Jefe de la Oficina TIC.
d. Todo software utilizado en los equipos propiedad de la Alcaldía del municipio de Fusagasugá, de los equipos conectados a la Red corporativa o que se utilicen en las instalaciones de la Alcaldía del municipio de Fusagasugá deben poseer las licencias de uso legal.
e. El traslado y movimiento de equipos debe ser realizado por la Oficina de Tecnologías de la Información y las Comunicaciones; la novedad debe ser registrada en el software de gestión de Oficina de Tecnologías de la Información y las Comunicaciones que use la Alcaldía del municipio de Fusagasugá.
f. No se permite la navegación a sitios Web de alto riesgo o que puedan comprometer la posición de la Alcaldía del municipio de Fusagasugá. Así mismo, la descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el desempeño de la Red corporativa.
g. El servicio de correo electrónico de la Alcaldía del municipio de Fusagasugá debe ser utilizado con propósitos laborales. Los usuarios son responsables de llevar una conducta ética y ajustada al ordenamiento legal cuando usen el correo electrónico. Así mismo, no se deben enviar correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la Red corporativa.
h. Los recursos de almacenamiento en Red que ha dispuesto la Alcaldía del municipio de Fusagasugá no deben ser utilizados para el almacenamiento de información que no sea para propósitos laborales.

6.3.4. Protección de la confidencialidad

Cada funcionario, contratista o personal tercerizado que haga uso de un activo de información debe seguir las siguientes instrucciones para preservar la Confidencialidad del activo correspondiente:

a. Verificar el nivel de clasificación del activo frente a Confidencialidad, esto se hace tomando como guía el ***Procedimiento de Clasificación y Etiquetado de la Información***
b. De acuerdo con la clasificación del activo frente a la Confidencialidad, el usuario que está accediendo a la información debe verificar que no tiene restricciones para

hacerlo de acuerdo con su Rol aplicando la Política de Control de Acceso; en caso contrario debe abstenerse de hacerlo e informar del hecho a su jefe inmediato y reportarlo como un incidente de seguridad de la información.

c. El usuario que accede a la información únicamente puede compartir dicha información con los usuarios que no tengan restricción para hacerlo, de acuerdo con la Política de Control de Acceso.
d. Se debe contar con la autorización expresa del encargado del área dueña de la información para suministrar o intercambiar información clasificada como Pública Clasificada y Pública Reservada a otras personas o entes externos.
e. Todos los funcionarios, contratistas o personal tercerizado de la Alcaldía del municipio de Fusagasugá están obligados a reportar como incidentes de seguridad de la información los accesos no autorizados a un activo de información de acuerdo con su clasificación.
f. No se permite el uso de software no autorizado o de propiedad de los usuarios en la plataforma tecnológica de la Alcaldía del municipio de Fusagasugá.

6.3.5. Protección de la integridad

Cada funcionario, contratista o personal tercerizado que haga uso de un activo de información debe seguir las siguientes instrucciones para preservar la Integridad del activo correspondiente:

- Verificar el nivel de clasificación del activo frente a Integridad, esto se hace tomando como guía el Procedimiento de Clasificación y Etiquetado de la Información.
- De acuerdo con la clasificación del activo frente a la Integridad, el usuario que está intentando modificar la información debe verificar que no tiene restricciones para hacerlo de acuerdo con su Rol aplicando la Política de Control de Acceso; en caso contrario debe abstenerse de hacerlo e informar del hecho a su jefe inmediato y reportarlo como un incidente de seguridad de la información.
- El usuario que modifique la información únicamente puede hacerlo, si la Política de Control de Acceso de la Alcaldía del municipio de Fusagasugá se lo autoriza.
- Todos los funcionarios de la Alcaldía del municipio de Fusagasugá están obligados a reportar como un incidente de seguridad de la información las modificaciones no autorizadas a un activo de acuerdo con su clasificación y a la Política de Control de Acceso de la Alcaldía del municipio de Fusagasugá.

6.3.6. Protección de la disponibilidad

Cada funcionario, contratista o personal tercerizado que haga uso de un activo de información debe seguir las siguientes instrucciones para preservar la Disponibilidad del activo correspondiente:

- Verificar el nivel de clasificación del activo frente a Disponibilidad, esto se hace tomando como guía el Procedimiento de Clasificación y Etiquetado de la

Información.

- De acuerdo con la clasificación del activo frente a la Disponibilidad, el usuario que haga uso del mismo debe validar que dicha acción no afecte el nivel de Disponibilidad del activo que debe ofrecer de acuerdo con el MSPI.
- Todos los funcionarios de la Alcaldía del municipio de Fusagasugá están obligados a reportar como un incidente de seguridad de la información el uso indebido de un activo que pueda afectar el nivel de Disponibilidad que debe ofrecer de acuerdo con el MSPI.
- El encargado del área dueña de la información junto con el oficial de seguridad de la información o quien haga sus veces, deberán propender porque las especificaciones físicas, técnicas y ambientales necesarias para la adecuada conservación de un activo de información sean cumplidas.

6.3.7. Devolución de los activos

Los funcionarios, contratistas o personal tercerizado deberán realizar la devolución formal de los activos de información asignados y/o desarrollados dentro de sus funciones al finalizar la relación contractual o laboral con la Alcaldía del municipio de Fusagasugá, o al presentarse un cambio de cargo, rol, área o responsabilidades.

6.3.8. Eliminación de medios

Se deberá asegurar que la información almacenada en medios lógicos o físicos, y que haya dejado de ser útil para la Alcaldía del municipio de Fusagasugá, sea debidamente eliminada utilizando la opción de borrado seguro con el uso de herramientas destinadas para este fin.

El papel impreso con información Pública Clasificada o Pública Reservada de la Entidad deberá ser destruido utilizando una trituradora de papel.

6.3.9. Inventario de activos

Se debe mantener y actualizar de forma regular un inventario clasificado de activos de información de la Alcaldía del municipio de Fusagasugá, designándose para cada uno un responsable y cuando aplique, un custodio del mismo, así como un nivel de acuerdo con su valoración en términos de la Confidencialidad, Integridad y Disponibilidad.

Para la identificación, inventario y clasificación de los activos de información se deberá usar el Procedimiento de Clasificación y Etiquetado de la Información de la Alcaldía del municipio de Fusagasugá.

6.4. POLÍTICA DE DESARROLLO SEGURO DE SOFTWARE

6.4.1. Objetivo de la política

La Política de Desarrollo Seguro de Software de la Alcaldía del municipio de Fusagasugá

busca asegurar que las consideraciones y controles relacionados con la seguridad de la información se encuentren diseñados e implementados dentro del ciclo de vida del desarrollo de software.

6.4.2. Declaración general de la política de desarrollo seguro de software

La Alcaldía del municipio de Fusagasugá establece que las aplicaciones y sistemas de información catalogados como críticos deben incluir en el ciclo de vida del desarrollo la aplicación de los criterios de seguridad de la información que hagan frente a las amenazas más difundidas en el entorno de las redes de datos.

6.4.3. Especificación de requisitos de seguridad

El máximo responsable del área o las áreas que van a ser usarías o propietarias del sistema, o de aquellas áreas propietarias de la información a la que el sistema va a tener acceso, junto con el oficial de seguridad de la información o quien haga sus veces, deberán promover para que se realicen los análisis y especificaciones funcionales de seguridad, antes de la fase de desarrollo.

Los mecanismos de seguridad que se implementen durante el desarrollo de un sistema deben ser proporcionales en costo y esfuerzo al perfil de riesgo de la información que accede, procesa y/o almacena el sistema.
Para especificar los requerimientos funcionales de seguridad se debe tener en cuenta lo establecido en las siguientes secciones.

6.4.4. Requerimientos funcionales de seguridad de la información

Protección de la Confidencialidad: Considerando la clasificación para los activos de información de la Alcaldía del municipio de Fusagasugá cada sistema desarrollado debe proveer los mecanismos para proteger la confidencialidad con base en el nivel al que pertenezca el activo que se va a proteger. En este sentido, los mecanismos mínimos que las aplicaciones desarrolladas para la Alcaldía del municipio de Fusagasugá deben proveer de acuerdo con el criterio de clasificación de la información según los descrito en el procedimiento de etiquetado y clasificación de la información son:

- **Cifrado de datos clasificados como confidenciales:** Opción de cifrar los datos en tránsito y almacenamiento con un algoritmo criptográfico que no tenga vulnerabilidades conocidas en el momento del desarrollo.
- **Control de acceso:** Mecanismos de autenticación y de gestión de roles y privilegios siguiendo la Política de control de acceso de la Alcaldía del municipio de Fusagasugá. Como mínimo se requiere autenticación por usuario y contraseña.
- **Registro:** Permitir la parametrización para generar el registro de eventos que permitan consignar los accesos a la información y así poder evidenciar potenciales violaciones a la confidencialidad de la misma.

Protección de la Integridad: Para proteger la integridad de la información los sistemas deben desarrollar como mínimo las siguientes utilidades, que serán aplicadas con base en la clasificación del activo de información que sea accedido, procesado y/o almacenado:

- **Control de acceso:** Aplica lo mismo que para la protección de la Confidencialidad.
- **Cifrado de datos:** Para la información clasificada en el nivel más alto de integridad se aplica el mismo cifrado contemplado para la protección de la Confidencialidad.
- **Verificación por Hashing**: Opción que permite validar la integridad de los datos de acuerdo con el criterio de clasificación de la información según los descrito en el procedimiento de etiquetado y clasificación de la información, los datos a verificar son los públicos clasificados o públicos reservados almacenados y/o transmitidos utilizando un campo de hashing que se genere con el algoritmo SHA que será calculado en la capa de acceso a datos con el uso de una librería válida. Este valor será almacenado hasta el momento en que se requiera la validación de integridad, momento en que se volverá a calcular el hashing y se realizará la comparación con el valor almacenado anteriormente.
- **Registro:** Permitir la parametrización para generar el registro de eventos que permitan auditar cuando se realizan cambios a la información.

Protección de la Disponibilidad: Para cumplir con los requerimientos de disponibilidad, las aplicaciones desarrolladas para la Alcaldía del municipio de Fusagasugá deben garantizar la aplicación de mejores prácticas relacionadas con manejo de excepciones, validación de entradas, controles criptográficos y gestión de sesiones.

Registro de eventos: Se recomienda que el registro de eventos se haga en el formato syslog, este debe incluir en su orden: fecha, hora, proceso, y descripción del evento.

Las aplicaciones de la Alcaldía del municipio de Fusagasugá deben contar con la opción de registrar al menos la información relacionada con siguientes eventos:

- Creación, modificación y/o eliminación de datos.
- Creación, modificación y/o eliminación de usuarios.
- Creación, modificación y/o eliminación de perfiles de usuario.
- Cambios en la configuración de la aplicación.

Información general del sistema:

- Desempeño de la aplicación incluyendo fecha y numero de versión. o Caídas o bloqueos del sistema o alguno de sus componentes. o Puesta en servicio del sistema.
- Detenciones manuales del servicio.
- Problemas de hardware.

De igual manera, los registros capturados deberán contar mínimo con los siguientes

datos:

- **Fecha y Hora:** Señalando el año, mes, día, hora y segundos de la recepción del requerimiento.
- **Usuario:** Identificación de la cuenta responsable de la acción.
- **Tipo de Requerimiento:** Señalar cuál fue la acción solicitada por el usuario.
- **Id:** Identificador de la sesión y de la transacción.**Tiempo de procesamiento computacional:** Intervalo de tiempo en el cual el usuario recibió la respuesta.
- **Alerta:** Registrar si durante la ejecución de la transacción se presentó alguna situación anormal. Es necesario implementar una función de manejo de excepción en las capas de presentación, lógica de negocio y acceso a datos para lograr capturar el código de error.
- **Exitosa técnicamente**: Saber si la transacción cumplió con el proceso y se dio una respuesta al usuario dentro del período de tiempo definido, esto se logrará registrar verificando si hay algún código de error.
- **Problema identificado:** Si la transacción no fue exitosa, especificar la causa correspondiente como problemas en la conexión, no hay respuesta de la Base de Datos, problemas en el enlace; se utilizará el mismo mecanismo descrito en el campo de Alerta.
- **Registro afectado:** ID del registro objetivo de la acción del usuario.
- **Base de Datos:** ID de la Base de Datos afectada por la acción del usuario
- **Tabla:** ID de la tabla afectada por la acción del usuario.
- **Dirección IP:** Desde donde se realizó el requerimiento. Esto dependerá de las limitantes que se puedan tener a nivel técnico inherentes a la tecnología utilizada.
- **Tamaño de la trama:** Registrar el tamaño del mensaje en bytes enviado para la solicitud
- **Tamaño de la trama de respuesta:** Registrar el tamaño del mensaje que la aplicación respondió.

Validación de datos de entrada: Para evitar que se encuentren vulnerabilidades de inyección o buffer overflow, que pueden posibilitar ataques de negación de servicio o acceso no autorizados, en el desarrollo de un sistema se tendrán en cuenta las siguientes consideraciones:

- **Protección contra buffer overflow:** Aplicación de las mejores prácticas en el desarrollo para tener un estricto control en la definición del tipo de variables para que se ajusten a los requerimientos. La validación se realiza analizando el código en cada una de las sentencias de definición de variables para que se limiten a un dominio o rango requerido por la función correspondiente. Un buffer overflow se presenta cuando se acepta como entrada grandes cantidades de caracteres que logran desbordar el segmento de datos y que adicionalmente con una longitud específica pueden llegar a un segmento privilegiado de la memoria, donde se pueden ejecutar ciertos comandos; es decir que el atacante debe encontrar esta longitud y adicionalmente definir el comando que lograría ejecutar. Considerando lo

anterior cada variable definida debe tener un tipo de datos limitado, preferiblemente definido por el programador y que los mecanismos sean diseñados para que solo capturen lo estipulado por los formatos aceptados o lo estrictamente requerido; si dentro de la revisión de código se evidencia que no se implementan estas restricciones, a pesar de que funcionalmente sea aprobado se está generando una vulnerabilidad.

- **Restricción de las capturas**: Los datos que se ingresen al sistema estarán restringidos por la longitud y el tipo de datos para limitar a lo estrictamente necesarios. La validación se realiza analizando el código para cada una de las sentencias de captura de datos, verificando que se realice la "sanitización" o validación que restrinja los valores que puedan ser ingresados. Para cada uno de los campos capturados se deben definir el tipo de datos que se va a capturar; la validación debe proceder para constatar que las capturas de datos validen que no se ingresen caracteres que puedan ser usados para una intrusión lo cual significa cadenas de texto que correspondan a "Comandos o instrucciones en los lenguajes o sistemas operativos involucrados", de esta forma el Programador debe considerar los filtros más exigentes posibles de tal forma que sin limitar datos validos restrinja palabras o meta caracteres que puedan ser usados en comandos o instrucciones. Se debe considerar que muchas veces los atacantes cambian las codificaciones (ASCII, EBCDIC, UNICODE) para evadir los controles.
- **Librerías:** Se tendrá una validación para evitar el uso de librerías con vulnerabilidades de cualquier tipo. La validación se realiza analizando el código y evaluando que cada una de las librerías utilizadas no tengan reporte de vulnerabilidades. Se tendrá una validación en el framework de desarrollo el cual alertará sobre las librerías que se encuentren obsoletas y así evitar el uso de componentes vulnerables para la aplicación. Las vulnerabilidades son catalogadas por los boletines emitidos por los fabricantes correspondientes.
- **Parámetros enviados a través de la URL:** Restringir el tamaño y el tipo de caracteres que son enviados en los parámetros de la URL para evitar ataques de Cross Site Scripting y la exploración no autorizada de directorios del servidor donde resida la aplicación. La validación se realiza analizando el código para cada una de las sentencias de captura de datos, verificando que se realice la validación que restrinja los valores que puedan ser ingresados.

- **Protección contra Inyecciones:** Las fallas de inyección, tales como SQL, OS, y LDAP, ocurren cuando datos no confiables son enviados a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al interprete para ejecutar comandos no intencionados o acceder a datos no autorizados. La mejor manera de averiguar si una aplicación es vulnerable a una inyección es verificar que en todo uso de intérpretes se separa la información no confiable del comando o consulta. Para llamados SQL, esto significa usar variables parametrizadas en todas las sentencias preparadas y procedimientos almacenados, evitando las consultas dinámicas. Verificar el código es una manera rápida y precisa para ver si la aplicación usa intérpretes de manera segura.

Control de sesión de usuarios: Se debe contar con la opción de definir un tiempo máximo de sesión de usuario, para ello se debe hacer uso de herramientas predefinidas en los diferentes entornos de desarrollo. También se debe establecer un control de memoria aplicando un reinicio de sesión por cada nueva solicitud en el menú o interface de usuario.

Manejo de excepciones en el desarrollo de software: En el desarrollo del sistema, para cada una de las funciones implementadas serán contempladas las opciones resultantes de los casos de abuso, es decir evitar que la aplicación pierda el control en el flujo posible de acciones, evitando que una excepción permita vulnerar los controles y las políticas de seguridad definidas. Todas las funciones tendrán un manejo específico para los casos que estén por fuera de los que señalan los requerimientos funcionales

6.4.5. Ambientes de desarrollo, prueba y producción

Se deben implementar y mantener separados los ambientes de desarrollo, pruebas y producción, de tal manera que el desempeño o las fallas en un ambiente no deberá afectar a los demás. En este sentido, los privilegios de acceso se deben diferenciar para cada uno de los ambientes, de tal manera que el personal de desarrollo o de pruebas no puedan ingresar al ambiente productivo.

El acceso al código fuente de los programas debe ser restringido, implementando controles de acceso y registros de auditoria para el ingreso, así como herramientas que permitan controlar los cambios realizados en el código para así detectar modificaciones no autorizadas.

El Jefe de la Oficina TIC coordinará para que todos los procesos se documenten y actualicen las reglas para la transferencia de software o actualizaciones entre cada uno de los ambientes de desarrollo, pruebas y producción.

6.5. POLÍTICA DE CONSTRUCCIÓN DE SISTEMAS SEGUROS

6.5.1. Objetivo de la política

La Política sobre Principios de Construcción de Sistemas Seguros de la Alcaldía del municipio de Fusagasugá busca asegurar que los sistemas de información sean diseñados, construidos, implementados, mejorados y mantenidos teniendo en cuenta las consideraciones de seguridad de la información que permitan proteger la Confidencialidad, Integridad y Disponibilidad de los activos de información de la Entidad.

6.5.2. Declaración general de la política de construcción de sistemas seguros

Los sistemas de información que la Alcaldía del municipio de Fusagasugá total o parcialmente adquiera, construya o contrate deberán ser diseñados, implementados, integrados, operados, actualizados, o y mantenidos teniendo en cuenta las mejores

prácticas vigentes de seguridad de la información y en cumplimiento de lo establecido por el MSPI de la organización.

6.5.3. Desarrollo seguro

La especificación, diseño, desarrollo y pruebas de cada uno de los componentes del sistema de información debe cumplir con la Política de Desarrollo Seguro de Software de la Alcaldía del municipio de Fusagasugá.

6.5.4. Proveedores

Los principios de construcción de sistemas seguros aquí establecidos deben aplicarse también a los sistemas de información externos a través de los contratos y otros acuerdos vinculantes entre la Alcaldía del municipio de Fusagasugá y el proveedor al que se subcontrata.

Estos principios no solo aplican para los proveedores, ya que algunas dependencias u oficinas muchas veces contratan personal para que realice desarrollos propios en la entidad (In House). Adicional a esto es importante que todos los principios no solo apliquen en la fase de construcción, sino también en las actualizaciones y/o nuevas versiones de los actuales sistemas de información de la entidad, por lo que en ocasiones las dependencias contratan el servicio de soporte, mantenimiento y actualización de acuerdo a las necesidades, cambios de ley o normatividad.

En este sentido se debe tener en cuenta lo que aplique desde la **Política de Seguridad de Proveedores** de la Alcaldía del municipio de Fusagasugá.

6.5.5. Identificación de activos de información

Los sistemas que se deban construir en la Alcaldía del municipio de Fusagasugá deben contemplar los niveles de Confidencialidad, Integridad y Disponibilidad de los activos de información con los que vayan a interactuar, para que de esta forma sean definidos los controles que cada sistema demande. Para cada caso se debe considerar lo siguiente:

- **Confidencialidad:** De acuerdo con el nivel de clasificación que tenga el activo de información que se encuentra en la matriz de activos de información, para esta propiedad de confidencialidad, se debe definir para el sistema de información, los mecanismos de control de acceso con base en la restricción del acceso a la información definida por la Alcaldía del municipio de Fusagasugá. Para los dos (2) niveles más altos es requerido la implementación del cifrado de datos directamente en las aplicaciones.
- **Integridad:** De acuerdo con el nivel de clasificación que tenga el activo de información para esta propiedad, se debe definir para el sistema de información los mecanismos de detección y/o control de modificaciones con base en la restricción

de cambios a la información definida por la Alcaldía del municipio de Fusagasugá, para los dos (2) niveles más altos de clasificación es requerido que se implemente los sistemas de verificación de integridad directamente en las aplicaciones.

- **Disponibilidad:** Con el nivel de clasificación que tenga el activo de información para esta propiedad, se debe definir para el sistema de información las copias de respaldo o mecanismos de redundancia de acuerdo con el nivel de criticidad.

6.5.6. Gestión de vulnerabilidades

Para cada componente del Sistema de Información se debe realizar un proceso de identificación y remediación de vulnerabilidades que debe incluir como mínimo los siguientes aspectos:

- **Monitoreo de amenazas:** Definir la responsabilidad por la revisión permanente del surgimiento de amenazas para aplicaciones que puedan afectar uno o más componentes del Sistema de Información.
- **Detección automatizada:** Implementar una herramienta de detección automática de vulnerabilidades que esté configurada con las firmas y patrones que puedan identificar proactivamente las vulnerabilidades para cada uno de los componentes del Sistema de Información.
- **Priorización:** Se debe priorizar la remediación de las vulnerabilidades de acuerdo a su criticidad y al perfil de riesgo del activo de información al cual afecten.
- **Generación de suplementos:** Definir la responsabilidad por la generación de los parches correspondientes a las vulnerabilidades identificadas, esto es las correcciones sobre el código para erradicar la falla encontrada.
- **Descarga de suplementos:** Para componentes desarrollados por fabricantes reconocidos, como por ejemplo los sistemas operativos, se debe definir la responsabilidad por la búsqueda y descarga de los parches liberados por los fabricantes.
- **Parches Virtuales:** Establecer el esquema de seguridad perimetral que contenga la firma de ataque o patrón identificado que busque aprovechar las vulnerabilidades identificadas; esto aplica en el lapso requerido para la generación o búsqueda del Parche correspondiente. Lo anterior se logra con sistemas de detección y prevención de intrusiones.
- **Aplicación de los Parches:** Realizar el proceso requerido para verificar que el parche a aplicar cumpla con su objetivo y no afecte la normalidad de la operación.
- **Verificación de la Remediación:** Una vez se realice la aplicación del parche se debe establecer una verificación del funcionamiento del sistema para corroborar que el parche cumple su objetivo y no afecta la normalidad de la operación.
- **Excepciones:** Las excepciones en la remediación de vulnerabilidades, esto es, los casos en que por distintas circunstancias del negocio o de la operación sea necesario asumir las vulnerabilidades técnicas, deben ser estudiadas por un comité de seguridad de la información y solo será el dueño del proceso al cual pertenezca la información comprometida quien pueda autorizar que vulnerabilidades

relacionadas con sus activos de información sean asumidas.

6.5.7. Monitoreo

Se debe definir los mecanismos para realizar el monitoreo del sistema de información siguiendo las siguientes directrices:

Registro de eventos (logs)

Se deben diseñar y configurar los componentes de los Sistemas de Información para que generen registros de auditoría de accesos y actividades de los usuarios y administradores aplicando los establecido al respecto en la Política de Desarrollo Seguro de Software de la Alcaldía del municipio de Fusagasugá; esto incluye entre otros a los sistemas operativos, bases de datos, servidores web, equipos de red, equipos de seguridad informática y a las aplicaciones.

El nivel de especificación o detalle requerido para el registro de eventos dependerá de los niveles de clasificación de la información involucrada. Los registros de auditoría generados por los componentes del Sistema de Información deberán contener la información suficiente para poder evidenciar en detalle las actividades, excepciones, y eventos ejecutados.

Es importante contar con un formato de control de cambios para los sistemas de información, de tal modo que pueda ser una fuente de información para la gestión del conocimiento. Este documento debe relacionar al detalle el cambio efectuado, pero adicional a ello generar la actualización del manual de usuario o guía para especificar los cambios que ha tenido la interfaz de usuario.

Protección de la información de los registros de eventos

Se deben implementar mecanismos para proteger la información correspondiente a los registros de eventos en cuanto a su Confidencialidad, Integridad y Disponibilidad.

En este sentido los registros de eventos deben ser almacenados con control de acceso, cifrados para las propiedades confidencialidad e integridad de la información y se les debe realizar copias de respaldo.

El oficial de seguridad de la información, o quien haga sus veces, en conjunto con el líder del proceso o encargado del área dueña de los activos de información involucrados, debe establecer el tiempo de retención de los registros, de conformidad con la normatividad aplicable.

El log debe ser limpiado, pues en las bases de datos, las tablas de logs tienden a crecer de manera exponencial de acuerdo al tipo de operaciones, por consiguiente, estos logs

deben estar bajo una supervisión y tal como lo señala la política estableciendo un periodo para que sean retenidos, según lo considere el líder del proceso dueño de la información.

Monitoreo del uso del sistema

Se deben establecer las funciones para el seguimiento en línea del sistema de información, esto es la revisión de los registros de eventos con los filtros correspondientes para el análisis de cierto tipo de información que puede requerir la toma de decisiones inmediatas. En este sentido, como mínimo se debe monitorear la disponibilidad del sistema, las alertas y fallas del sistema, los accesos privilegiados y los bloqueos por detección de abusos sobre el sistema (por ejemplo, el bloqueo por exceso de intentos fallidos de autenticación).

Es relevante efectuar el seguimiento para evidenciar los casos de disponibilidad del sistema, alertas y fallas del sistema, para descartar posible ataques internos o externos

Sincronización del reloj

La Oficina de Tecnologías de la Información y las Comunicaciones por medio de cada administrador de la plataforma, deberá establecer mecanismos de sincronización y verificación del reloj para todos los dispositivos que hacen parte de la plataforma tecnológica que soporte esta configuración, de acuerdo con la normatividad vigente.

6.5.8. Gestión de incidentes de seguridad de la información

Todo funcionario, contratista o tercera parte debe reportar los Incidentes de Seguridad de la Información de la Alcaldía del municipio de Fusagasugá. En resumen, se requiere el desarrollo de las siguientes funcionalidades:

- **Identificación de Anomalías:** Para cada componente de un Sistema de Información se debe determinar cuál es el patrón de comportamiento normal para reportar oportunamente cualquier tipo de evento que rompa con dicho patrón. Estos patrones de comportamiento se basan en umbrales mínimos y máximos por protocolo, aplicación, origen y destino, entre otros; también pueden hacer uso de la detección de tipos y estructuras de mensajes o tipos y estructuras de protocolos.

- **Evaluación de anomalías:** Una vez se identifica una anomalía se debe establecer el mecanismo para evaluar si dicha anomalía corresponde a un incidente de seguridad, para esto es necesario la verificación general del Sistema de Información para verificar si se pudo comprometer la Confidencialidad, Integridad y/o Disponibilidad de la información.

- **Tratamiento de incidentes:** Una vez se detecta el incidente se deben establecer los mecanismos para reaccionar oportunamente y reducir el alcance o impacto de la amenaza que logró materializarse. Para este propósito es necesario clasificar los

tipos de incidente y determinar que propiedad de la seguridad se afectó, así como el nivel de criticidad del o los activos involucrados, y sobre esta base decidir las acciones correspondientes.

Se deben construir, administrar y mantener reportes que registren los incidentes de seguridad de la información que se presenten, los cuales deben contener toda la información técnica recopilada del incidente y de la actividad de respuesta al mismo. Estos reportes deben ser protegidos contra accesos no autorizados.

Cualquier recolección de datos relacionados con un incidente, los cuales puedan considerarse útiles como elementos probatorios para ser tenidos en cuenta dentro de una investigación, deberá ser llevada a cabo garantizando siempre la cadena de custodia.

6.5.9. Seguridad de red

El Sistema de Información debe contar con una protección a nivel de red que incluya las siguientes funcionalidades:

- **Segmentación:** Se debe separar en segmentos de Red diferentes los componentes del Sistema de Información que tengan diferente nivel de criticidad, así por ejemplo los equipos de usuario no pueden estar en el mismo segmento en que se encuentren los servidores de base de datos.
- **Firewall:** Los responsables del desarrollo del Sistema de Información deben entregar los puertos que son utilizados por los componentes o aplicaciones y las direcciones IP origen y destino, para que de esta forma se configuren las reglas correspondientes en el Firewall.
- **IDS:** Los responsables del desarrollo del Sistema de Información, sean proveedores o funcionarios, en conjunto con el Oficial de Seguridad de la Información, o quien haga sus veces, deben definir periódicamente cuales son las firmas de ataque y patrones anómalos que deben ser identificados para tomar una acción con base en alguna situación de riesgo.
- **IPS:** Considerando el punto anterior, el administrador del Sistema de Información, apoyado por el Oficial de Seguridad de la Información de la Alcaldía del municipio de Fusagasugá o quien haga sus veces, debe decidir cuáles de las firmas de ataque y/o patrones anómalos deben ser bloqueados automáticamente.
- **VPN:** Se debe implementar este tipo de conexión que protege los datos con mecanismos de cifrado y verificación de integridad para la información que así lo establezca el plan de tratamiento de riesgos del MSPI.
- **DLP:** Se debe implementar herramientas que protejan la información sensible de los Sistemas de Información ante intentos de transmisión o copiado no autorizados.

6.5.10. Gestión de capacidad

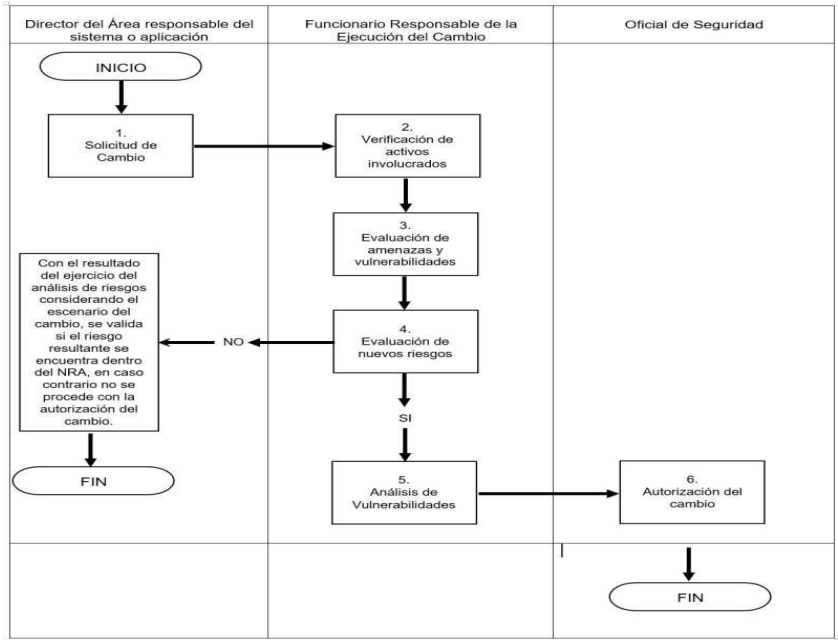
El máximo responsable del área dueña de la información debe coordinar con la Oficina de

Tecnologías de la Información y las Comunicaciones las proyecciones de crecimiento del volumen de información y transacciones dentro de los objetivos misionales de su área, para que sea posible planificar a tiempo la capacidad de los Sistemas de Información involucrados.

Con la información recopilada durante la interacción con el encargado del área dueña de la información, la Oficina de Tecnologías de la Información y las Comunicaciones será la responsable de aplicar las acciones pertinentes para mantener los niveles adecuados de capacidad, y deberá establecer y aplicar los procedimientos e instructivos de gestión de capacidad.

6.5.11. Control de cambios en sistemas de información

Durante la realización de cambios en los Sistemas de Información de la Alcaldía del municipio de Fusagasugá se deben aplicar los siguientes pasos:



a. La Oficina de Tecnologías de la Información y las Comunicaciones en cabeza del jefe de la Oficina TIC debe definir los instructivos y procedimientos específicos a seguir para realizar cambios sobre los Sistemas de Información y la plataforma tecnológica de la Alcaldía del municipio de Fusagasugá, incluyendo el análisis de riesgos previo a una puesta en producción.
b. El líder del proceso que sea dueño de la información es el responsable de aprobar los cambios a realizarse en los Sistemas de Información que interactúen con la información a su cargo.

c. Cualquier cambio en la plataforma tecnológica y/o en los Sistemas de Información de la Alcaldía del municipio de Fusagasugá deberá ser completamente documentados por parte de los ingenieros encargados y antes deben ser aprobados por el líder del proceso o dueño de la información.

d. Se deben realizar pruebas funcionales a los Sistemas de Información una vez se ejecuten cambios sobre los mismos. La aceptación de los resultados de dichas pruebas es responsabilidad del líder del área dueña de la información, quien también debe asegurarse porque se actualice la documentación funcional relacionada.

e. La Oficina de Tecnologías de la Información y las Comunicaciones será responsable de realizar pruebas de seguridad y otras pruebas no funcionales a los Sistemas de Información luego de cambios realizados en sus componentes, y verificará que se actualice la documentación de seguridad y la documentación técnica relacionada.

6.5.12. Respaldo de la información

Se deben establecer y documentar procedimientos y/los instructivos para el respaldo de los datos de los Sistemas de Información de acuerdo con lo establecido por la Política de Generación y Restauración de Copias de Respaldo de la Alcaldía del municipio de Fusagasugá.

6.5.13. Cumplimiento legal y regulatorio

De acuerdo con el marco legal y regulatorio aplicable a la Alcaldía del municipio de Fusagasugá el desarrollo del Sistema de Información debe considerar los siguientes lineamientos:

- **Licenciamiento:** Este documento debe ser revisado y aprobado por el Jefe de la Oficina Asesora Jurídica de la Alcaldía del municipio de Fusagasugá. En caso de ser un desarrollo interno o contratado, dicho documento debe elaborarse con base en los lineamientos de la Oficina Asesora Jurídica de la Alcaldía del municipio de Fusagasugá.
- **Datos Personales:** Si el sistema de información incluye el manejo de datos personales, este debe aplicar la Política de Protección de Datos Personales de la Alcaldía del municipio de Fusagasugá.
- Se recomienda la lectura mandatoria del Protocolo PT-GT-001 del proceso GESTIÓN TIC, en especial en el Anexo 01 de ese documento.

6.6. POLÍTICA DE GENERACIÓN Y RESTAURACIÓN DE COPIAS DE RESPALDO

6.6.1. Objetivo de la política

La Política de Generación y Restauración de Copias de Respaldo de la Alcaldía del municipio de Fusagasugá provee las directrices para que el proceso de generación y restauración de copias de respaldo se realice aplicando los requerimientos de seguridad para los activos de información.

6.6.2. Declaración general de la política de generación y restauración de copias de respaldo

La Alcaldía del municipio de Fusagasugá establece que las copias de respaldo se deben ejecutar como mínimo para todos los activos de información clasificados en los niveles medio y alto de disponibilidad, aplicando una estrategia que tenga en cuenta los puntos y tiempos de recuperación adecuados para cada tipo de información, manteniendo durante el tránsito y almacenamiento de la copia los requerimientos de seguridad establecidos para el activo original y asegurando mediante pruebas periódicas la consistencia y capacidad de recuperación de los respaldos.

6.6.3. Obligatoriedad del respaldo

Se establece que toda información que sea utilizada o generada dentro de los procesos y procedimientos formalmente definidos en la Alcaldía del municipio de Fusagasugá deben contar con un mecanismo de respaldo para salvaguardar la información.

En este sentido, cada activo de información va a ser respaldado de acuerdo con unas necesidades puntuales que dependerán de su clasificación, su perfil de riesgo y los requerimientos legales y normativos que le apliquen. Los máximos responsables de cada proceso en coordinación con cada funcionario deben determinar la necesidad puntual del respaldo, es decir, para que se va a usar. Algunos escenarios pueden ser, entre otros:

- Respaldar la información para restaurar los datos en caso de un desastre, crisis o incidente.
- Respaldar la información para recuperar un archivo en caso de supresión o la corrupción del mismo.
- Respaldar la información para almacenar datos históricos.
- Respaldar la información para dar cumplimiento a estándares y/o mejores prácticas.
- Respaldar la información para para dar cumplimiento del marco legal y regulatorio.

6.6.4. Estrategia de respaldo

Se debe definir una estrategia de respaldo para los diferentes tipos de activos de información, la cual debe contemplar los requerimientos surgidos de las necesidades puntuales, de los diferentes escenarios de respaldo, y de las consideraciones de seguridad de la información, entre otros aspectos.

Para la definición de la estrategia de respaldo pueden participar diferentes dependencias de la Alcaldía del municipio de Fusagasugá, pero la aprobación final la debe dar el máximo

responsable del área dueña de la información, y la implementación se debe hacer en forma coordinada con la Oficina de Tecnologías de la Información y las Comunicaciones la cual ayudará a dimensionar la solución y guiará en como documentar los instructivos de respaldo y recuperación dependiendo de las tecnologías que se seleccionen.

Por lo tanto, la implementación, solución y documentación de los instructivos de respaldo y recuperación es un trabajo articulado con los demás procesos y la Oficina de Tecnologías de la Información y las Comunicaciones.

Los requerimientos que pueden surgir, y que se deben por tanto determinar para definir la estrategia y dimensionar la solución de respaldo son:

- **Tiempo objetivo de recuperación (RTO):** Corresponde al tiempo máximo de inactividad tolerable por la Entidad a partir de la declaración del evento adverso que afecte la disponibilidad de determinada información o sistema. Para una copia de respaldo representa el tiempo necesario, desde la ocurrencia del evento adverso, para que la copia sea restaurada y se tenga acceso nuevamente a la información
- **Punto objetivo de recuperación (RPO):** Define la máxima cantidad de datos que una Entidad tolera perder en la ocurrencia de un evento adverso que afecte la disponibilidad de determinada información. Para una copia de respaldo dependerá de la última vez que se tomó dicha copia antes del evento adverso.
- **Disponibilidad:** Para los sistemas de información se debe establecer cuál es el porcentaje de disponibilidad del mismo requerido en un periodo de tiempo dado considerando la criticidad del proceso que atiende. Esto se define con base en los tiempos límite de indisponibilidad exigidos para cada una de las actividades donde está involucrado el activo de información.
- **Confidencialidad:** En el caso de la información clasificada como confidencial o pública reservada se deberá implementar el cifrado en los medios de respaldo, y deberá estar protegida contra accesos y restauraciones no autorizadas.
- **Retención:** Existe cierta información que por cumplimiento de regulaciones y legislaciones debe ser retenida en medios por una cantidad de tiempo determinada. Se tendrá en cuenta esta particularidad a la hora de dimensionar las soluciones de respaldo, así como lo dispuesto en las tablas de retención documental de la Entidad.
- **Plan de Continuidad del Negocio:** Para la información o las aplicaciones que se respalda como parte de una estrategia de continuidad del negocio, se deben tener en cuenta las ubicaciones físicas de las copias y el medio de respaldo más conveniente. Se deben tener en cuenta los resultados del BIA (Bussines Impact Analisis, por sus siglas en inglés) para definir lo que se va respaldar y la manera en se va a hacer.
- **Condiciones medioambientales de los medios de respaldo**: Se debe dar un nivel adecuado de protección física y medioambiental a los medios de respaldo, en su trasporte y almacenamiento, tanto en los sitios principales como en los de contingencia, conforme a lo establecido por los fabricantes y la normatividad vigente.

- **Presupuesto:** Estará definido con base en la criticidad de los activos de información involucrados, con lo cual se dispondrá de mayores recursos para aquellos que lo justifiquen. En cuanto a una copia de respaldo esto se verá reflejado en una mayor inversión en los siguientes aspectos:

✓ Tecnología utilizada. o Frecuencia de la copia de respaldo (definida por el RPO).
✓ Cantidad de respaldos completos con respecto a los diferenciales.
✓ Límite de espacio antes de la sobre escritura en los medios de respaldo.
✓ Pruebas de las copias de respaldo.

6.6.5. Pruebas

Las copias de respaldo deben ser probadas periódicamente por la Oficina de Tecnologías de la Información y las Comunicaciones para corroborar que los datos fueron tomados y almacenados correctamente y llegarán a ser consistentes y usables cuando los originales sufran un evento adverso.

Las pruebas deben realizarse cumpliendo con el siguiente protocolo base:

- Se deben ejecutar las pruebas al menos trimestralmente.
- Realizar la restauración sobre un ambiente de pruebas.
- Llevar a cabo actividades que se realizan normalmente sobre los datos en este ambiente de pruebas para verificar su consistencia.
- En caso de encontrarse anomalías realizar el reporte del Incidente
- Si las pruebas son exitosas debe guardarse el registro para corroborar el buen estado de la copia de respaldo en algún formato o bitácora que se debe crear a la media de la solución que se adquiera.

6.6.6. Responsabilidad de los usuarios

Los funcionarios, contratistas y personal tercerizado serán responsables del respaldo de la información relacionada con su función institucional contenida en los equipos de cómputo a su cargo, para lo cual deben coordinar con la Oficina de Tecnologías de la Información y las Comunicaciones, en cabeza del Jefe de la Oficina TIC, para que les provea los recursos y herramientas necesarias para hacer el respaldo y la restauración, de lo contrario cada proceso tendría una herramienta diferente y no compatible con los demás procesos.
Cada proceso debe crear registros de control que permita llevar un historial de los funcionarios que hacen copias de seguridad de la información, la dependencia (fechas, tamaño, entre otros), esta información debe ser de pleno conocimiento de los dueños de proceso y deben efectuarse por diversas novedades, es decir no solo por la periodicidad establecida en la política sino por asuntos como retiro del cargo temporal o definitivo, licencias, vacaciones, comisiones, entre otros.

Los funcionarios, contratistas y personal tercerizado deberán verificar constantemente que

las herramientas de respaldo en sus equipos estén activadas y no presenten alertas. En el caso de encontrar anomalías, deberán reportarlas como un evento de seguridad de la información.

6.7. POLÍTICA DE USO DE DISPOSITIVOS MÓVILES

6.7.1. Objetivo de la política

La Política de Uso de Dispositivos Móviles de la Alcaldía del municipio de Fusagasugá, busca mantener la seguridad de la información cuando se haga uso de dispositivos móviles por parte de los funcionarios y contratistas de la entidad en el ejercicio de sus funciones misionales, sin importar si estos son de propiedad del funcionario o contratista para cumplir sus funciones laborales.

6.7.2. Declaración general de la política de uso de dispositivos móviles

La Alcaldía del municipio de Fusagasugá establece que el uso de dispositivos móviles por parte de sus funcionarios para el acceso, almacenamiento o procesamiento de información de la entidad está por defecto restringido, y solo podrá autorizarse mediante aprobación y responsabilidad expresa del dueño del proceso en cual desempeñe sus funciones, actividades u obligaciones la persona que haría uso del dispositivo móvil. Una vez aprobado su uso, se debe informar al Oficial de Seguridad de la información, o quien haga sus veces.

La información creada, procesada, almacenada o accedida en o desde el dispositivo móvil debe contar con los controles establecidos de acuerdo con su clasificación, tal como se haría en los demás equipos de la entidad, aplicando para su protección las mismas restricciones y condiciones explícitas en las demás políticas de seguridad de la información.

6.7.3. Uso aceptable de dispositivos móviles

El uso de dispositivos móviles por parte de los funcionarios y contratistas de la Alcaldía del municipio de Fusagasugá para el acceso y manejo de información de la Entidad está permitido siempre y cuando se cumpla con lo establecido en la presente política.

Para tales efectos, se considera que un dispositivo móvil está siendo usado para acceder o manejar información de la Alcaldía del municipio de Fusagasugá cuando se utiliza para alguna o varias de las siguientes actividades:

a. Recepción, envío o lectura de correo electrónico corporativo.
b. Almacenamiento o visualización de documentos e información propios de la Alcaldía del municipio de Fusagasugá.
c. Acceso a los sistemas de información, aplicaciones o portales Web que exijan autenticación y sean propias de la Alcaldía del municipio de Fusagasugá.
d. Acceso directo a una red inalámbrica de la Alcaldía del municipio de Fusagasugá.
e. Acceso a una VPN de la Alcaldía del municipio de Fusagasugá desde cualquier otra

Red.

f. Conexión vía cable USB, bluetooth, wifi, o cualquier otra, a equipos de cómputo propiedad de la Alcaldía del municipio de Fusagasugá o en los cuales pueda existir información o acceso a información de la Alcaldía del municipio de Fusagasugá.
g. Toma de fotografías o videos relacionados con la actividad de la Alcaldía del municipio de Fusagasugá.
h. Grabación de audio de actividades relacionadas con la misión de la Alcaldía del municipio de Fusagasugá.
i. Establecimiento de chats, video llamadas, llamadas, mensajes de texto, y en general cualquier comunicación, en la que se discutan temas relacionados con información de la Alcaldía del municipio de Fusagasugá.

En todos estos casos, la información procesada en el dispositivo móvil debe contar con los controles establecidos de acuerdo con su clasificación de la información, tal como se haría en los demás equipos de la Red de la Alcaldía del municipio de Fusagasugá, y aplican para su protección las mismas restricciones y condiciones explícitos en las demás políticas de seguridad de la información. Adicionalmente, se deben considerar las amenazas inherentes a la condición de portabilidad de los dispositivos móviles, como son el robo, daño, conexión a redes inalámbricas potencialmente maliciosas y uso no autorizado.

En este sentido, se establece que para el uso de todo dispositivo móvil que acceda, almacene, procese o sea origen de información de la Alcaldía del municipio de Fusagasugá clasificada en los niveles Público Clasificado y Público Reservado de Confidencialidad, así como Medio y Alto de Integridad y Disponibilidad, se deben asegurar unas condiciones de manejo mediante la firma de un Acuerdo de Uso por parte del propietario y/o usuario del dispositivo móvil. El acuerdo debe diseñarse por parte de la Alcaldía del municipio de Fusagasugá con apoyo del proceso jurídico.

6.7.4. Acuerdo de uso

Documento que redacta el uso aceptable del dispositivo móvil cuando se conecte a los sistemas de información o aplicaciones de la Alcaldía del municipio de Fusagasugá, estableciendo las responsabilidades y las directrices que deben ser seguidas por los funcionarios y contratistas que hagan uso de dispositivos móviles. Se debe tener en cuenta:

a. Que el funcionario o contratista debe firmar el acuerdo de uso del dispositivo móvil previo a su activación en la red de la Entidad para hacer labores que tengan que ver con sus funciones en la entidad.
b. La firma de dicho documento debe renovarse anualmente.
c. El funcionario o contratista debe firmar el acuerdo cuando cambie el dispositivo.

El acuerdo contiene los siguientes elementos:

a. Definir claramente la responsabilidad sobre el plan de voz y datos por el cual está

cubierto el dispositivo, si lo hace la Entidad o el funcionario o contratista, así como los términos de dicho plan.

b. Se aplicarán las políticas de seguridad de la información de la Alcaldía del municipio de Fusagasugá.
c. El funcionario o contratista debe hacer el reporte de la pérdida o robo del dispositivo cuando este incidente ocurra. Este plazo es de máximo 4 horas para equipos propiedad de la Alcaldía del municipio de Fusagasugá y 24 horas para equipos propios de los funcionarios o contratistas.
d. En el caso de equipos propiedad de la Alcaldía del municipio de Fusagasugá, el funcionario o contratista debe hacer un uso razonable del dispositivo para que entre otras cosas este no tenga funcionalidades por fuera de lo relacionado con el trabajo, como son entre otros: juegos, música, videos diferentes a los institucionales, apuestas y uso de redes sociales para fines diferentes a los institucionales.
e. En el caso de equipos propiedad del funcionario o contratista, se debe permitir, y ser técnicamente viable en ese dispositivo, la segregación de la información, aplicaciones, y los entornos de sistemas operativos relacionados con el uso personal y de trabajo.
f. El funcionario o contratista no revelará o permitirá el acceso a terceros no autorizados a información almacenada en el dispositivo.
g. El funcionario o contratista se hace responsable de mantener el equipo en las condiciones requeridas para desarrollar su trabajo, completando las reparaciones requeridas en un plazo razonable.
h. Tener habilitado el control remoto para borrado de todos los datos y programas en caso de pérdida o robo del dispositivo.
i. Aceptar el tener habilitado el control remoto desde una herramienta de administración centralizada para borrado de todos los datos y programas en caso de pérdida o robo del dispositivo.
j. Configurar las reglas de contraseña de acuerdo con la política de control de acceso de la Alcaldía del municipio de Fusagasugá.
k. Permitir monitorear intentos de desbloqueo.
l. Permitir el borrado del dispositivo después de un número determinado de intentos fallidos de acceso.
m. Activar el bloqueo de pantalla con contraseña después de un tiempo de desuso o por activación manual.
n. Manejar una vigencia de la contraseña de acceso acorde con las políticas de la Alcaldía del municipio de Fusagasugá.
o. Uso controlado de las diferentes formas de grabación disponibles como son voz, cámaras de video y fotográfica, evitando registros no autorizados o que vayan en contra de la Legislación Colombiana.
p. El dispositivo deberá soportar del software de cifrado definido por la Alcaldía del municipio de Fusagasugá.
q. Soporte del dispositivo a la descarga, actualización o borrado de aplicaciones.
r. Permitir a la herramienta de administración centralizada la Alcaldía del municipio de Fusagasugá el habilitar o deshabilitar el WiFi.

s. El funcionario o contratista deberá realizar o permitir la instalación del antimalware definido por la Alcaldía del municipio de Fusagasugá.
t. Se deberán instalar siempre las actualizaciones del antimalware.
u. Aislar el equipo cuando esté comprometido por malware o un acceso no autorizado.
v. Eliminar las aplicaciones que sean consideradas maliciosas o inapropiadas.
w. Permitir la implementación y monitoreo de herramientas DLP cuando aplique, incluyendo la posible instalación de agentes.
x. Permitir la auditoría del dispositivo por parte de la Alcaldía del municipio de Fusagasugá.
y. Realizar copias de respaldo de la información allí contenida acorde con el procedimiento de copias de respaldo establecido por la Alcaldía del municipio de Fusagasugá.

6.7.5. Verificación

a. Revisión periódica de los acuerdos firmados donde se verifique fecha, cargo y firma, validando la vigencia del documento frente al MSPI.
b. Al menos una vez al año, se debe proceder con un proceso de revisión del equipo móvil para verificar que se encuentre acorde con las políticas establecidas.
c. Anualmente se deberán sensibilizar a los funcionarios y contratistas por parte de la Oficina de Tecnologías de la Información y las Comunicaciones en temas de seguridad de la información asociados al uso de este tipo de tecnologías.

6.7.6. Información procesada en el dispositivo móvil

a. Cada activo de información almacenada, transmitida y accedida, o de alguna forma procesado en un dispositivo móvil debe cumplir con los requerimientos de seguridad de la información definidos en el MSPI de la Alcaldía del municipio de Fusagasugá.
b. Se debe establecer una carpeta donde únicamente se almacenen y procesen datos personales del usuario. Esta carpeta será excluida de las acciones correspondientes a auditoría y seguimiento.

6.8. POLÍTICA DE TRASFERENCIA DE LA INFORMACIÓN

6.8.1. Objetivo de la política

La Política para la Transferencia de Información de la Alcaldía del municipio de Fusagasugá provee las directrices para que todos los procedimientos o procesos que involucren transferencia de información se lleven a cabo protegiendo la confidencialidad y la Integridad de la misma, utilizando para ello los mecanismos acordes con el nivel de clasificación que corresponda.

6.8.2. Declaración general de la política de trasferencia de información

La Alcaldía del municipio de Fusagasugá establece que la trasferencia de información digital, tanto interna como externa, puede realizarse solo a través de los medios definidos y suministrados para tal fin por la entidad, o por un cliente o proveedor en el caso que la Alcaldía así lo acuerde, aplicando los controles necesarios para proteger la confidencialidad, integridad y disponibilidad de los activos de información que sean objeto de la trasferencia con base a su clasificación.

6.8.3. Generalidades

Previo a ser trasferidos, los activos de información deben haber pasado por un proceso de clasificación de la información aplicando el Procedimiento de Clasificación y etiquetado de la Información de la Alcaldía del municipio de Fusagasugá.

En ese orden de ideas, la transferencia de Información debe realizarse protegiendo la Confidencialidad y la Integridad de los datos con los mecanismos que se encuentren establecidos en el MSPI de la Alcaldía del municipio de Fusagasugá de acuerdo con la clasificación del activo de información involucrado.
Para la entidad la clasificación de la información se encuentra en una matriz de identificación de activos de información, donde se encuentra valorada cada propiedad de la seguridad de la información.

6.8.4. Formas de transferencias aceptadas

Para la Alcaldía del municipio de Fusagasugá las formas de transferencia de datos formalmente aceptadas y reconocidas son las siguientes:

- Correo electrónico. Ejemplos de correos que se originan en la entidad pero que tienen destinatarios diferentes a los de la alcaldía.
- Protocolos de Transferencia de archivos, incluyendo herramientas de transferencia segura de información. Ejemplos de herramientas son el ftp, el ftp seguro, ssh, winscp y mozilla entre otros.
- Repositorios compartidos. Ejemplo cuando un usuario copia un archivo publico reservado o publico clasificado hacia carpetas de otras compañías o hacia herramientas que permitan transferencia de archivos, pero cuya información se origine en las carpetas o repositorios compartidos. Lo ideal es que la información de tipo publico reservado o publico clasificado este cifrada antes de transferirse.

Aunque la copia de archivos a través de medios removibles es una forma de transferencia de información, esta se aborda en el Procedimiento de Gestión de Medios Removibles.

No está permitida la trasmisión de información clasificada en los niveles Público Reservado y Público Clasificado de Confidencialidad, o Medio y Alto de Integridad, a través de utilitarios o sistemas de mensajería instantánea, llamadas o video llamadas que usen plataformas públicas, ni a través de la red telefónica IP o de videoconferencia de la Alcaldía

del municipio de Fusagasugá.

Los usuarios deben utilizar los medios de transferencia aceptados solo para temas relacionados con la misión de la Alcaldía del municipio de Fusagasugá y con sus labores institucionales, y cumpliendo las políticas del MSPI que apliquen para cada caso y etapa de la transmisión.

6.8.5. Protección de la confidencialidad y la integridad

Previo a la transferencia de la información se debe aplicar la protección de la confidencialidad y la integridad de los datos, aplicando cifrado o el Procedimiento de Transferencia de información.
En los casos que se haga uso de un protocolo de transmisión que soporte algoritmos criptográficos, esto reemplazará el uso del procedimiento señalado.

6.8.6. Protección de la disponibilidad

Las herramientas tecnológicas que se provean deben estar avaladas por el proceso de "Tecnologías de la Información y las Comunicaciones" quien debe certificar que la herramienta designada valida que el medio de comunicación ofrecido para la Transferencia de la Información cumple con el nivel de disponibilidad exigido, para lo cual se deben evaluar los siguientes aspectos:

- **Bandwith (Ancho de banda):** Es la capacidad del canal de transferencia de información y que establece la cantidad de datos que pueden ser transmitidos por unidad de tiempo.
- **Delay (Retraso):** El tiempo requerido para la transmisión entre dos puntos de la red.
- **Jitter (Fluctuación):** Es la fluctuación que puede presentarse en la señal de transmisión y que tiene como consecuencia directa un retraso en la transmisión. Jitter puede definirse también como las variaciones en el Delay (retardo).
- **Pérdida de Paquetes:** Es el porcentaje de paquetes perdidos en las transferencias de datos.

Estos aspectos deben ser registrados formalmente en cada uno de los enlaces requeridos para transferencia de información determinando cuales son los valores permitidos para poder cumplir con el nivel de disponibilidad que se exige para la Transferencia del activo de información involucrado.

6.8.7. Registro de la transferencia

Las transferencias de información realizadas por medios electrónicos deben ser registradas en los servidores correspondientes almacenando los siguientes datos referentes al evento:

- Fecha

- Hora
- Dirección IP origen
- Dirección IP Destino
- Usuario que envía
- Usuario que recibe
- Transmisión exitosa / fallida
- Tamaño de los datos transmitidos
- Protocolo utilizado
- Algoritmo de cifrado o firmado

Para ello se debe exigir, durante la especificación de los requerimientos correspondientes, que en la arquitectura de los sistemas desarrollados o implementados en o para la Alcaldía se incluyan las funcionalidades de registro de eventos de auditoria directamente en las aplicaciones, incluyendo el almacenamiento y protección de dichos registros. En este sentido, se debe tener en cuenta las directrices establecidas al respecto en las políticas de desarrollo seguro y de construcción de sistemas seguros de la entidad.

El proceso de “Tecnologías de la Información y las Comunicaciones” debe certificar que la herramienta designada que utilizarán los usuarios cumple con los mecanismos para ejercer el registro y control de los datos que requieren capturarse del evento de transferencia.

6.8.8. Interconexión en sistemas de información

La arquitectura de interconexión entre los diferentes componentes de los sistemas de información de la Alcaldía del municipio de Fusagasugá debe tener en cuenta la protección de la Confidencialidad y de la Integridad de los datos que se intercambian, de acuerdo con la clasificación de la información y a las políticas del MSPI de la Alcaldía del municipio de Fusagasugá.

6.8.9. convenios de intercambio

Cuando exista un intercambio de información con entes externos y/o terceras partes, el mismo deberá cumplir con lo establecido en la presente política, para lo cual se deberá contar con los convenios establecidos que tengan en cuenta los requerimientos de seguridad de la información, con base en la clasificación de la información que se va a intercambiar.

Estos convenios deben ser autorizados por el dueño de la información, y deben ser formalmente acordados en los compromisos contractuales. Entre otros aspectos, los convenios tendrán en cuenta lo siguiente:

a. Las responsabilidades para controlar y notificar la transmisión, envío y recepción de información.
b. Los Procedimientos para garantizar la trazabilidad y el no repudio.
c. El uso de un sistema de etiquetado acordado para la información, de acuerdo con

el Procedimiento de Clasificación y Etiquetado de Información de la Alcaldía del municipio de Fusagasugá.

d. Cumplimiento de lo establecido en la Política de control de acceso de la Alcaldía del municipio de Fusagasugá.
e. Cumplimiento de la legislación y regulaciones vigentes que apliquen para la Alcaldía del municipio de Fusagasugá.

6.8.10. Manejo de excepciones

Debe ser provista la información correspondiente a la ocurrencia de anomalías en el proceso de transferencia de datos, a continuación, se citan algunos casos sin limitarse a estos:

- Congestión de la Red.
- Indisponibilidad del destino.
- Paquetes malformados.
- Bloqueo por comportamiento anómalo.
- Bloqueo por firma de ataque.
- Bloqueo por dirección IP origen.
- Bloqueo por dirección IP destino.

En estos casos cabe la posibilidad de incluir fallas en los equipos de red o medios de transmisión, operador del servicio de internet, entre otros.

6.9. POLÍTICA DE SEGURIDAD PROVEEDORES

6.9.1. Objetivo de la política

La Política de Seguridad de Proveedores de la Alcaldía del municipio de Fusagasugá provee las directrices para que los activos de información que sean manejados por proveedores y terceras partes estén cubiertos por las Políticas de Seguridad de la información de la Entidad.

6.9.2. Declaración general de la política de seguridad proveedores

La Alcaldía del municipio de Fusagasugá establece que la relación con sus proveedores debe siempre estar definida en un acuerdo mutuo que establezca específicamente la protección de la confidencialidad, integridad y disponibilidad de los activos de información que estén involucrados en el desarrollo del servicio o producto contratado; este acuerdo siempre debe estar en un contrato formal acorde con la legislación colombiana.

6.9.3. Cumplimiento de las políticas de seguridad de la información

Las Políticas de Seguridad de la Información de la Alcaldía del municipio de Fusagasugá son de obligatorio cumplimiento para toda persona que realice labores como proveedor de la Entidad, independiente del área o compañía a la cual pertenezca y cualquiera sea el

nivel de las tareas que desempeñe.

Así mismo, los funcionarios de la Alcaldía del municipio de Fusagasugá que interactúen con un proveedor, o que sean responsables de la supervisión de su actividad, deben tomar conciencia acerca de los temas relacionados con la seguridad de la información, y serán los responsables por que el proveedor cumpla las políticas de seguridad de la información y porque se utilicen los controles pertinentes y se sigan los procedimientos definidos antes, durante, y después de la relación contractual con dicho proveedor.

6.9.4. Acuerdos de confidencialidad

Toda relación contractual que establezca un proveedor o personas que sean contratadas para la prestación de servicios de apoyo, servicios técnicos, servicios especializados, asesores y consultores con la Alcaldía del municipio de Fusagasugá, deberá incluir un acuerdo de confidencialidad.

Este acuerdo de confidencialidad debe ser revisado por el área jurídica y debe ser firmado sin excepción alguna con cualquier proveedor con el que se establezca cualquier tipo de intercambio de información, y debe señalar que la información a la que tenga acceso el proveedor como parte del servicio prestado a la Alcaldía del municipio de Fusagasugá solo puede ser conocida por las personas y/o entidades que estén formalmente autorizadas.

Este acuerdo también trae consigo las penalizaciones con base en los daños potenciales ante la violación de la confidencialidad de la información.

6.9.5. Protección de datos personales

Se debe incluir dentro del contrato con el proveedor una cláusula que haga referencia al cumplimiento de la Política de Protección de Datos Personales de la Alcaldía del municipio de Fusagasugá, documento que debe ser entregado al proveedor para su entendimiento y aceptación.

6.9.6. Personal encargado del servicio

El funcionario responsable por parte de la Alcaldía del servicio o proyecto donde se involucre uno o más proveedores debe validar que todos los funcionarios de las compañías proveedoras que tengan acceso a información de la entidad, estén vinculados contractualmente con dichas compañías.

6.9.7. Gestión de incidentes

Es obligación por parte de los funcionarios de la empresa proveedora el reporte de cualquier anomalía que sea detectada para que su tratamiento sea oportuno y se prevengan incidentes de seguridad de la información. De la misma forma, los

supervisores de los contratos y los líderes de los procesos serán responsables por reportar como un evento de seguridad de la información cuando se observen situaciones en las acciones del proveedor que atenten contra la seguridad de la información (Integridad, Confidencialidad, Disponibilidad) en los servicios o productos suministrados.

6.9.8. Control y auditoria

El máximo responsable del proceso dueño de la información deberá propender, con el apoyo del Oficial de Seguridad de la Información o quien haga sus veces, porque las acciones sobre la información de la Alcaldía del municipio de Fusagasugá que realicen los proveedores generen registros de auditoría. Estos registros deben ser almacenados al menos por el tiempo que dure la relación contractual.

6.9.9. Requerimientos de seguridad de la información

Si el proveedor es responsable por aplicaciones o servicios informáticos estos deben cumplir con los requerimientos de protección de la Confidencialidad, Integridad y Disponibilidad definidos por la Alcaldía del municipio de Fusagasugá, y que debe demostrar con base en el activo que va a ser manejado con uno o más de los siguientes controles:

- **Monitoreo:** Estar en capacidad de brindar los mecanismos para detectar incidentes de seguridad de la información sobre el funcionamiento de la aplicación con el que se presta el servicio a la Alcaldía del municipio de Fusagasugá. El nivel de detección se ajustará a los requerimientos del activo involucrado en el servicio.
- **Gestión de Vulnerabilidades:** Mantener un proceso de revisión permanente de las posibles vulnerabilidades en las aplicaciones que son responsabilidad del proveedor, con el fin de mitigar oportunamente los riesgos asociados con las vulnerabilidades identificadas.
- **Control de acceso:** Presentar los mecanismos de control de acceso a los servicios y los datos manejados con base en la Política de Control de Acceso de la Alcaldía del municipio de Fusagasugá.
- **Gestión de incidentes:** Contar con un esquema de identificación, reporte, escalamiento, tratamiento y documentación de los incidentes que se presenten en el funcionamiento de la aplicación o servicio prestado.
- **Soporte:** El proveedor debe contar con los expertos idóneos para atender incidentes o eventos de seguridad de la información con base en el Modelo de Seguridad y Privacidad de la Información de la Alcaldía del municipio de Fusagasugá.
- **Redundancia:** Si los servicios provistos así lo requieren, el proveedor debe contar con sistemas redundantes que le permitan cumplir con los acuerdos de niveles de servicio acordados con la Alcaldía del municipio de Fusagasugá.
- **Licenciamiento:** Todas las aplicaciones y servicios prestados por el proveedor deben contar con el licenciamiento acorde con el marco legal y regulaciones que apliquen a la Alcaldía del municipio de Fusagasugá.

Para permitir la supervisión por parte de la Alcaldía de los controles anteriormente expuestos, se debe incluir en los requisitos contractuales que el proveedor acepte someterse a auditorías externas por parte de la Alcaldía cuando la entidad lo disponga; aportando durante dichas auditorías las certificaciones y/o documentación que le sean requeridos para demostrar los controles que ha implementado para las aplicaciones, sistemas e información o servicios informáticos que le presta a la entidad.

6.9.10. Requerimientos de seguridad de la información de la empresa proveedora

La Alcaldía del municipio de Fusagasugá exigirá unas condiciones mínimas con respecto a Seguridad de la Información para las empresas proveedoras con las que exista intercambio de información catalogada en los niveles Pública Clasificada y Pública Reservada de Confidencialidad, así como Alto de Integridad y Alto de Disponibilidad, a saber:

- Contar con una implementación mínima del modelo de seguridad de la información.
- Presentar la política de seguridad de la información referente al servicio o producto que se está prestando a la Alcaldía del municipio de Fusagasugá.
- Mostrar sus procedimientos de gestión de vulnerabilidades y diagnóstico de seguridad.
- Mostrar los planes de contingencia y recuperación donde muestre su capacidad de cumplir con la disponibilidad exigida en los acuerdos de niveles de servicio.
- Presentar los procedimientos o instructivos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.
- Presentar la documentación de los controles físicos y lógicos empleados por el tercero para proteger la confidencialidad, integridad, disponibilidad de los datos y los equipos.

Las empresas proveedoras cuyos servicios incluyen aspectos controlados por la legislación o regulaciones vigentes aplicables a la Alcaldía del municipio de Fusagasugá, deben asegurar y demostrar su cumplimiento.

6.9.11. Requerimientos de seguridad de la información de personas naturalescomo proveedores

Las personas que actúen como proveedores de la Alcaldía del municipio de Fusagasugá, deberán seguir las Políticas de seguridad de la información definidas para los funcionarios, teniendo como única excepción lo relacionado con el proceso disciplinario, que en este caso hará alusión a un Incumplimiento de Contrato.

6.10. POLÍTICA DE BLOQUEO DE PUERTOS

6.10.1. Objetivo de la política

La política de bloqueo de puertos de la Alcaldía del municipio de Fusagasugá busca proteger la información que se encuentran dentro de un computador, ya sea de contagio de virus o plagio de la misma

6.10.2. Declaración general de la política de bloqueo de puertos

Todos los funcionarios de la alcaldía del municipio de Fusagasugá son responsables del manejo de la información que manejan en sus respectivos equipos, para la trasmisión, envió o copia de su información, el único medio utilizado es de manera impresa, el correo electrónico o el drive de correo, ya que con el manejo de una unidad de almacenamiento como lo es una memoria flash (USB) o una unidad de DVD, el computador está expuesto a infectarse de virus y debido a esto una posible pérdida de la información.

6.10.3. Privilegio del uso de los puertos

Los privilegios de uso de los puertos que se definan se deben basar en las funciones y responsabilidades del cargo o rol que desempeñe el funcionario, contratista o personal de planta dentro de la entidad

6.10.4. Permisos para el uso de los puertos

La activación para el uso de los puertos, solo puede ser dada o autorizada por el jefe de la oficina tic, para dicha activación el funcionario, contratista u oficial de planta debe pasar un oficio en donde especifique el porqué de la activación de los puertos y el uso destinado que se le va dar, ejemplo, copia y traslado de la información o grabación de información en un DVD.

6.10.5. Bloqueo de puertos USB

La configuración de los equipos de la alcaldía de Fusagasugá, depende, exclusivamente de que el equipo se encuentre en el dominio de la entidad, ya estando en dicho dominio, toda configuración se lleva a cabo por medio del Directorio Activo, configuraciones como por ejemplo el bloqueo y activación de puertos USB, la creación de usuarios, acceso a la red de internet, funciones y privilegios exclusivos que tiene cada funcionario, contratista u oficial de plana debido a sus actividades contractuales

6.11. POLÍTICA DE LEGISLACIÓN APLICABLE Y REQUISITOS CONTRACTUALES

6.11.1. Objetivo de la política

Evitar el incumplimiento por parte de la Alcaldía del municipio de Fusagasugá de las obligaciones legales, reglamentarias o contractuales relacionadas con la seguridad de la información.

6.11.2. Declaración general de la política de legislación aplicable y requisitos contractuales

La Alcaldía del municipio de Fusagasugá establece como mandatorio para todas sus actividades el cumplimiento de las leyes, obligaciones estatutarias, reglamentarias y cualquier requisito enmarcado en la legislación colombiana, así como los requisitos contractuales que establezca con sus proveedores, relacionados con la seguridad de la información, evitando así acarrear sanciones administrativas, que puedan incurrir en responsabilidad civil, penal o disciplinaria como resultado de su incumplimiento.

6.11.3. Cumplimiento de los requisitos legales

Considerando el marco legal y regulatorio colombiano a continuación se hace referencia a las diferentes leyes y decretos que aplican a la Alcaldía del municipio de Fusagasugá en lo relacionado a seguridad de la información y que por tanto deben ser contemplados para que los datos sean clasificados y tratados acorde con las restricciones y/o limitaciones que imponga este marco legal.

6.11.4. Constitución

Con respecto a la protección de la confidencialidad de la información, se deben considerar todos los datos que dentro de la Constitución aparecen como de Carácter Reservado.

6.11.5. Ley general de archivo

Es la Ley 594 de 2000 y/o cualquier otra que la derogue, la cambie o la sustituya, cuyo objetivo es establecer las reglas y principios generales que regulan la función archivística del Estado; los procesos y los Sistemas de Información de la Alcaldía del municipio de Fusagasugá deben cumplir con estos lineamientos. Cabe destacar que dentro del artículo 27 se declara que todas las personas tienen derecho a consultar los documentos de archivos públicos y a que se les expida copia de los mismos, siempre que dichos documentos no tengan carácter reservado conforme a la Constitución o a la ley.

6.11.6. Protección de datos personales

En lo referente a datos personales, en el marco Legal Colombiano se encuentran la Ley 1581 de 2012 sobre la Protección de Datos Personales y/o cualquier otra que la derogue, la cambie o la sustituya, así como la Ley 1266 de 2008 y/o cualquier otra que la derogue, la cambie o la sustituya que junto con la sentencia T729 de 2002 tratan el principio de Habeas Data.

Para dar cumplimiento a esta legislación se recomienda revisar los documentos del proceso GESTIÓN TIC como Manual para el uso adecuado de la infraestructura tecnológica MA-

GT-001 y Protocolo de servicios informáticos y compromiso de confidencialidad sobre tratamiento de datos PT-GT-001

6.11.7. Ley de trasparencia

Es la Ley 1712 de 2014 y/o cualquier otra que la derogue, la cambie o la sustituya cuyo objeto es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información. Los procesos y sistemas de información de la Alcaldía del municipio de Fusagasugá deben responder a esta ley cumpliendo con el principio de Disponibilidad para todos los datos que apliquen.
Para asegurar el cumplimiento de esta Ley la Alcaldía del municipio de Fusagasugá cuenta con el liderazgo del Jefe de la Oficina TIC.

6.11.8. Estrategia de gobierno en línea

La Estrategia de Gobierno en línea en Colombia ha evolucionado considerando los significativos avances de la Tecnología, así como también los resultados y las tendencias mundiales en gobierno electrónico. Esta evolución permitirá a las entidades públicas adaptarse más fácilmente a las necesidades de la ciudadanía. La Estrategia actual se define en el Decreto único reglamentario del Sector de las Tecnologías de la Información y las Comunicaciones 1078 de 2015, uno de sus propósitos es garantizar la seguridad y privacidad de la información.

Para dar cumplimiento a la estrategia GEL la Alcaldía del municipio de Fusagasugá cuenta con el liderazgo del Jefe de la Oficina TIC. Actualmente la Oficina TIC es la secretaría técnica del comité GEL, pero el liderazgo lo asume quienes están en el comité representando a la Alcaldía.

6.11.9. Protección de derechos de autor

Al respecto, en Colombia se cuenta con el siguiente marco legal:

- Constitución Política de 1991, en su artículo 61, que expresa: “El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley”.

- Decisión 351 de 1993, o Régimen Común Andino sobre Derecho de Autor y derechos Conexos, es de aplicación directa y preferente a las leyes internas de cada país miembro del Grupo Andino.

- Ley 23 de 1982 de Propiedad Intelectual y/o cualquier otra que la derogue, la cambie o la sustituya, contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia.
- Ley 44 de 1993 y/o cualquier otra que la derogue, la cambie o la sustituya, modifica

y adiciona la Ley 23 de 1982.

6.11.10. Ley 1273 de 2009

La Ley 1273 de 2009 y/o cualquier otra que la derogue, la cambie o la sustituya, modificó el código penal, creando un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos”, y busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Esta Ley tipificó como delitos una serie de conductas relacionadas con el manejo de la información y los datos personales, con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

6.11.11. Ley 734 de 2002

Esta Ley y/o cualquier otra que la derogue, la cambie o la sustituya, es por la cual se expide el Código Disciplinario Único, y a través de la cual el Estado ejerce su potestad sancionatoria para asegurar la obediencia, la disciplina y el comportamiento ético, la moralidad y la eficiencia de los servidores públicos, con miras a asegurar el buen funcionamiento de los diferentes servicios a su cargo.

7. UBICACIÓN DE LAS POLÍTICAS Y PROCEDIMIENTOS DENTRO DEL MSPI

A continuación, se presenta la lista de Políticas y Procedimientos que componen el MSPI de la Alcaldía del municipio de Fusagasugá:

1. El primer paso es la clasificación del activo de información, el cual se lleva a cabo utilizando el Procedimiento para la clasificación y el etiquetado de la información (A.8.2.3)
2. Una vez clasificada la información se debe aplicar la Etiqueta correspondiente utilizando el Procedimiento para la clasificación y el etiquetado de la información (A 8.2.2)
3. Como antesala a cualquier acción que se ejecute dentro de la Entidad debe ser considerada la Política de legislación aplicable y requisitos contractuales (A.18.1.1), y se debe aplicar el Procedimiento de verificación para el cumplimiento legislativo (A.18.1.2)
4. Con el etiquetado definido y la verificación legal, se procede a la aplicación de la Política de control de acceso a la información (A.9.1.1).
5. Para el caso del software, el punto de ingreso hacia el MSPI debe hacerse aplicando la Política de desarrollo seguro de software (A.14.2.1).
6. Implementar el esquema que aplique para el respaldo de la información aplicando la Política de generación y restauración de copias respaldo (A.12.3.1).
7. Para cualquier cambio que se requiera considerando la dinámica de la Entidad se debe aplicar el numeral 11.5 de este documento respecto del control de cambios.
8. Una vez se han aplicado las políticas y procedimientos de los puntos anteriores,

viene todo lo relacionado con el procesamiento y uso diario de los activos por parte de los funcionarios y con base en los requerimientos se aplican según sea el caso las siguientes:

a. En general para el manejo de los recursos de tecnología de información y comunicaciones por parte de todos los funcionarios se aplican la Política de uso aceptable de los activos (A.8.1.3).
b. Para los usuarios que manejen computadores portátiles, tabletas y/o teléfonos móviles se aplica la Política de uso de Dispositivos móviles (A.6.2.1)
c. Para todos los usuarios que hagan uso de un recurso informático se aplica la Política de escritorio limpio y pantalla limpia (A.11.2.9)
d. Cualquier tipo de transferencia de datos interna o externa se llevará a cabo cumpliendo la Política de transferencia de información (A.13.2.1) o numeral 11.8 de este documento con el correspondiente Procedimiento de transferencia de información (A13.2.1)
e. El manejo de medios de almacenamiento externo se regirá por el Procedimiento de gestión de medios removibles (A 8.3.1)
9. Cualquier incumplimiento por parte de los funcionarios y contratistas activa el Proceso disciplinario A7.2.3 (Código Único Disciplinario)
10. Para el caso de la información manejada con proveedores debe aplicarse la Política de seguridad de la información para relaciones con proveedores (A.15.1.1)

8. REFERENCIAS

Anexo 1, Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones, FEBRERO 2021

Documento maestro del modelo de Seguridad y Privacidad de la Información, Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones, OCTUBRE 2021

Roles y Responsabilidades, Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones, OCTUBRE 2021

9. CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DEL CAMBIO REALIZADO
01	01/2019	CREACIÓN DEL DOCUMENTO
02	01/2020	Aplicación de mejoras por QA
03	01/2021	Aplicación de las observaciones emitidas por la Alcaldía de Fusagasugá
04	01/2022	Aplicación de las mejoras emitidas por la Alcaldía de Fusagasugá

05	30/01/2023	Aplicación de las mejoras emitidas por la Alcaldía de Fusagasugá
06	**19/12/23**	**Ajuste según lo establecido en la guía elaboración de documentos y creación**

		de la política de bloqueo de medios removibles