# POLITICA DE SEGURIDAD DE LA INFORMACION

**ALCALDÍA FLORIDABLANCA**
**SANTANDER**

**TABLA DE VERSIONES**

| Versión | Fecha | Autor |
|---|---|---|
| **01** | 12/10/2020 | Dirección de Gobierno Digital |
| | | |
| | | |

# POLITICA DE SEGURIDAD DE LA INFORMACION

**SE ESTABLECEN:**

**PARAMETROS DE LA POLITICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION DEL MUNICIPIO DE FLORIDABLANCA**

## INTRODUCCIÓN

Los flujos en información, la posibilidad de materialización de siniestros informáticos, además de las normativas existentes exigidas por el Gobierno Nacional, son factores que impulsan la adopción de política, normas y según el caso procedimientos de seguridad de la información, todo ello para lograr tener un modelo de seguridad acorde a la necesidad de la institución.

Para ello debemos tener en cuenta la normatividad vigente en Colombia expuesta a continuación:

- Artículo 15 de la Constitución Política, consagra el derecho fundamental de las personas a conservar su intimidad personal y familiar, al buen nombre y a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en bancos de datos y en archivos de las entidades públicas y privadas.

- Ley 1273 de 2009 por medio del cual se modifica el Código Penal, crea un nuevo bien jurídico tutelado denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las

tecnologías de la información y las comunicaciones "TIC", entre otras disposiciones

- CONPES 3854 de 2016 se fijó la política Nacional de seguridad digital, para que las entidades del Estado constituyan mecanismos para la gestión de los riesgos digitales.

Y teniendo en cuenta la norma técnica NTC-ISO/IEC 27001:2013 y el habilitador de seguridad de la información de gobierno digital del Ministerio de Tecnologías de la Información y la Comunicaciones, se debe establecer una política general de seguridad de la información, políticas y procedimientos de seguridad de la información para salvaguardar y proteger los activos en sus tres pilares: Confidencialidad, Integridad y Disponibilidad.

## OBJETIVO

Formular la política general de la seguridad de la información, políticas y procedimientos de la seguridad de la información en la alcaldía municipal de Floridablanca - Santander, basado en la norma NTC-ISO-27001:2013, que le permita a la entidad la toma de decisiones para la seguridad y privacidad de la información.

### Específicos:

- Establecer, implementar y monitorear el modelo de seguridad y privacidad de la información o sistema de gestión de seguridad de la información en la alcaldía municipal de Floridablanca - Santander.
- Establecer y regular las actividades y labores relacionadas con la seguridad y privacidad de la información al interior de la organización.

## ALCANCE

La política de Seguridad de la Información comprende todas las secretarías y oficinas de la administración municipal, a sus servidores públicos, contratistas y terceros que manejen y/o generen información.

## DEFINICIONES

**Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

**Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

**Mejor Práctica:** Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

**Guía:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

**Procedimiento:** Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

## MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos".
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 1008 de 2018 ""Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- Artículo 61 de la Constitución Política de Colombia.
- Decisión Andina 351 de 1993. - Derechos de Autor
- Código Civil, Artículo 671. - PROPIEDAD INTELECTUAL. Las producciones del talento o del ingenio son una propiedad de sus autores.
- Ley 23 de 1982. – Derechos de Autor
- Ley 44 de 1993. – Derechos de Autor

## POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Dirección de Gobierno Digital de la alcaldía de Floridablanca, entendiendo la importancia de una adecuada gestión de la información y de acuerdo al decreto 1008 del 14 de junio de 2018 del Ministerio de Tecnologías de la Información y las Comunicaciones, establece que es necesario preservar la confidencialidad, integridad y disponibilidad de los activos de información de cada proceso de la organización, es por ello que se ha comprometido con la implementación de un modelo de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en

el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

La alcaldía municipal de Floridablanca se compromete a proteger los activos de información de cada proceso, de acuerdo a su criticidad para minimizar los impactos financieros y legales.

La alcaldía municipal de Floridablanca, se compromete a identificar y establecer controles para mitigar los diferentes riesgos que puedan afectar los activos de información y la continuidad de algún proceso de la alcaldía municipal de Floridablanca.

De acuerdo con lo anterior, esta política aplica a nuestra Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la alcaldía
- Garantizar la continuidad del negocio frente a incidentes.

## POLITICAS DE SEGURIDAD DE LA INFORMACION

## Política de protección de datos y privacidad de la información

Definir los lineamientos para la protección de datos y privacidad de la información de datos personales de la Alcaldía Municipal de Floridablanca.

La Alcaldía Municipal de Floridablanca realizará procesos de recolección, almacenamiento, procesamiento, uso y transmisión (según corresponda) de datos personales, atendiendo de manera estricta los postulados de seguridad y confidencialidad postulados en la Ley 1581 de 2012 y el Decreto 1377 de 2013. Teniendo en cuenta lo postulado con anterioridad, se definieron los siguientes lineamientos:

- La Alcaldía Municipal de Floridablanca reconoce que el único medio autorizado para el tratamiento de datos personales es el dueño de la información, de acuerdo a la Ley de protección de datos personales 1581 de 2012 y el decreto 1377 o la que la adicione, modifique o derogue.

- La Alcaldía Municipal de Floridablanca se compromete a otorgar los recursos necesarios para garantizar los tres (3) pilares fundamentales de la seguridad como son la disponibilidad, integridad y confidencialidad de la información, con el fin de dar cumplimiento a los objetivos institucionales, la estrategia y misión de la entidad.

- La Administración Municipal se compromete a cumplir con todos los requisitos legales, reglamentarios y contractuales que haya a lugar, con el fin de gestionar y reducir los riesgos a un nivel aceptable.

- Establecer la mejora continua del sistema de gestión de seguridad de la información, a través de un conjunto de reglas y directrices orientadas a garantizar la protección de los activos de información de la Alcaldía Municipal de Floridablanca, de una manera contundente, eficiente y efectiva, de la misma forma velar por tomar las acciones necesarias para la evaluación, análisis y tratamiento de los riesgos de acuerdo a la metodología adoptada por la Administración.

- La Dirección de Gobierno Digital se compromete a velar por la aplicación y cumplimiento adecuado de la presente política de seguridad de la información y todas las que se deriven de ella, por parte de todos los funcionarios, contratistas, colaboradores y terceros de la Alcaldía Municipal de Floridablanca.

- En cualquier situación que se deba realizar el tratamiento de la información personal de algún ciudadano y/o servidor público, se deberá contar con el consentimiento por escrito al titular de los datos para realizar el ejercicio y tener un registro del mismo.

- Se deberá conservar la información bajo condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- En caso tal que la información obtenida contenga datos erróneos, se deberá notificar de inmediato y realizar las correcciones correspondientes en el menor tiempo posible.

- Se deberá garantizar al dueño de la información, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

- Se deberá informar con prontitud cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los servidores públicos.

## ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Esta política tiene como finalidad establecer el comité directivo de la seguridad de la información. Debe tener los siguientes elementos: procdimiento de reuniones

¿Quiénes conforman el comité directivo de seguridad de la información?

**Objetivos**: Se deben especificar los objetivos del comité como por ejemplo el mejoramiento continuo de los programas o las distintas actividades que se realizarán en dichos comités, verificación de avance de los distintos proyectos, la revisión del documento de la política de seguridad .

**Cumplimiento:** Debe establecerse que dicho comité verifique el cumplimiento de las políticas.

### Política pantalla y escritorio limpio

Establecer los estándares para prevenir el riesgo de acceso no autorizado, pérdida, robo o modificación de la información durante y después de horas laborales.

**Pantalla limpia**:

- Las personas que trabajan o laboran en la Alcaldía Municipal de Floridablanca, deben bloquear, suspender o apagar los equipos tecnológicos (impresoras, equipos de cómputo, escáner y portátiles) cuando no estén en uso.

- La pantalla se debe conservar limpia, libre de información, que pueda ser utilizada por personas externas y sin autorización para su uso.

- El fondo de pantalla de los equipos de cómputo y portátiles de la Alcaldía Municipal de Floridablanca es establecido por la Dirección de Gobierno Digital.

- Cada equipo de cómputo y portátil que se encuentre en el dominio de la Alcaldía Municipal de Floridablanca cuenta con un tiempo establecido para el bloqueo de la pantalla cuando no se encuentre en uso.

- Los equipos de cómputo o portátiles se pueden bloquear o suspender utilizando las teclas Windows + L, o las teclas CTRL + ALT + SUPR - bloquear.

- Cada equipo de cómputo y portátil que se encuentre en el dominio de la Alcaldía Municipal de Floridablanca cuenta con un sistema de autenticación por usuario y contraseña establecido por la Dirección de Gobierno Digital.

**Escritorio limpio**:

- Las personas que trabajan o laboran en la Alcaldía Municipal de Floridablanca, cuando se ausenten del puesto de trabajo o después del horario laboral deben guardar los documentos o medios de almacenamiento removibles (USB, CD, Discos duros o DVD) que contengan información confidencial o clasificada de la entidad en un gabinete o escritorio con llave.

- Los documentos o medios de almacenamiento removibles (USB, CD, Discos duros o DVD) que se encuentren sin uso o desatendidos se deben guardar.

- Los documentos con información confidencial o clasificada se deben retirar de la impresora, fotocopiadora, escáneres y/o fax.

- Evitar escribir o dejar a la vista las contraseñas de acceso a sistemas, aplicaciones o equipos de cómputo.

**Política control de acceso físico**

Definir los lineamientos para el control de acceso físico en áreas seguras de la Alcaldía Municipal de Floridablanca.

- Las áreas seguras, dentro de las cuales se encuentran el datacenter, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, centros de datos físicos y digitales, áreas de procesamiento de información, entre otros, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

- Para el acceso a áreas seguras de la Administración Municipal se manejan accesos por medio de clave, huella, carnet institucional o permisos especiales según corresponda.

- Cada dependencia es responsable de designar a funcionarios y/o contratistas con los permisos de acceso a zonas restringidas en su área, llevando el control y seguimiento de los mismos.

- Todas las entradas que utilizan sistemas de control de acceso deben permanecer cerradas y es responsabilidad de todos los funcionarios, contratistas, colaboradores y terceros autorizados, como medida de seguridad, evitar que las puertas se dejen abiertas.

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

- Se deben realizar acciones para prevenir la pérdida, daño, robo o compromiso de activos de información y la interrupción de las operaciones de la organización; los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas, peligros del entorno y las posibilidades de acceso no autorizado, protegidos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro, el cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debe estar protegido contra interceptación, interferencia o daño.

**Política de acceso a redes y servicios en red.**

Definir los lineamientos clave para el acceso a redes y servicios en red de la Alcaldía Municipal de Floridablanca.

- La Dirección de Gobierno Digital suministra a los usuarios las contraseñas de acceso a los servicios de red, servicios y sistemas de información que requiera para el desempeño de sus funciones laborales.

- Las claves para el servicio de red inalámbrico están disponibles para los funcionarios y son suministradas por parte del equipo y previa autorización del Director de Gobierno Digital.

- Las claves para los servicios en red son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.

- Sólo el personal designado por la Dirección de Gobierno Digital está autorizado para configurar la red, instalar software o hardware en los equipos, servidores e infraestructura de tecnología de la Alcaldía Municipal de Floridablanca.

- Toda actividad que requiera acceder a los servidores, equipos o a las redes de la Alcaldía Municipal de Floridablanca, se debe realizar en las instalaciones y con el personal especializado. No se debe realizar ninguna actividad de tipo remoto sin la debida autorización la Dirección de Gobierno Digital.

- La creación y retiro de usuarios en los sistemas de información en producción debe seguir un procedimiento de creación, edición y estado de baja de usuarios.

- Toda actividad de red se controlará mediante los software y disposiciones dadas por el equipo de Gobierno Digital. donde se realizará el proceso de filtrado web, control de aplicaciones y antivirus perimetral.

- No existe una red de invitados (inalámbrica) habilitada para el acceso a todo público.

**Política seguridad en oficinas, recintos e instalaciones**

Gestionar los lineamientos básicos para la seguridad en oficinas, recintos e instalaciones de la Alcaldía Municipal de Floridablanca.

- Se debe establecer un control de acceso al público estricto para toda oficina, recinto e instalación clave (esta característica se define por el tipo de información y equipos tecnológicos con los que cuente cada área) para la Administración Municipal.

- Para toda oficina, recinto o instalación de la Administración Municipal que realicen actividades de procesamiento de información (manejo de información sensible) se deberán desarrollar estrategias para mostrar un indicio mínimo del propósito del área, con el fin de generar discreción en los procesos que se lleven a cabo y disminuir posibles intrusiones.

- Se debe tener un control estricto del directorio interno de extensiones de las oficinas de la Administración Municipal, es prioridad de los servidores públicos velar

por mantener seguras las extensiones de áreas sensibles (Datacenter, oficinas que generan información de alta criticidad, entre otras).

- Los perímetros de seguridad para oficinas, recintos e instalaciones de la Administración Municipal que manejen o generen información sensible (bases de datos, archivos, almacenes, etc.) deben estar delimitados por una barrera, como una pared, puerta de acceso controlado por un dispositivo de autenticación o una oficina de recepción, atendida por personal de la Administración Municipal que controle el acceso físico a estas áreas.

- Los puestos de trabajo de los funcionarios de la Administración Municipal deberán permanecer limpios y libres de documentación sensible y/o clasificada cuando se encuentren fuera de horario laboral o en ausencia prolongada del sitio, lo anterior con el fin de evitar accesos no autorizados a la información.

- Las personas que trabajan o laboran en la Alcaldía Municipal de Floridablanca, son responsables de bloquear, suspender o apagar los equipos tecnológicos (impresoras, equipos de cómputo, escáner y portátiles) cuando no estén en uso. Al finalizar actividades laborales, se deberán cerrar todas las aplicaciones y dejar los equipos respectivamente apagados.

- Los documentos con información confidencial o clasificada se deben retirar de la impresora, fotocopiadora, escáneres y/o fax para evitar la pérdida o robo de información de estos documentos.

**Política gestión de incidentes de seguridad de la información**

Gestionar de manera adecuada los eventos, incidentes y vulnerabilidades de seguridad de la información que se generen en la alcaldía municipal de Floridablanca con el fin de prevenir y limitar el impacto de los mismos.

Los lineamientos para reportar incidentes se encuentran definidos en el procedimiento para reportar incidentes de seguridad.

## Política instalación de software

Definir las directrices para la instalación de software en los equipos de la Alcaldía Municipal de Floridablanca para su correcto funcionamiento.

- La Dirección de Gobierno Digital deberá proporcionar el software que se requiera en los equipos de la Administración Municipal para el respectivo cumplimiento de las actividades laborales a desarrollar.

- Sólo personal capacitado y autorizado por la Dirección de Gobierno Digital se encargará de la instalación, actualización y monitoreo de los software que estén instalados en los equipos de la Administración Municipal.

- Todo software que se instale en los equipos de la Administración Municipal deberán contar con su licencia correspondiente (exceptuando casos de software libre), así como es responsabilidad de la Dirección de Gobierno Digital de mantener las licencias al día.

- Para el control de los programas que se instalen en los equipos de la Administración Municipal, la Dirección de Gobierno Digital deberá monitorear cada equipo de cómputo con una herramienta especial para dicho proceso.

- Si alguna dependencia de la Administración Municipal solicita un software en específico para el funcionamiento de su área, se deberá realizar la solicitud formal al jefe de Dirección de Gobierno Digital a través de un oficio, donde especifique el software requerido (el pago de la respectiva licencia de software se hace por parte de la dependencia que lo solicita).

## Política controles criptográficos

Definir las directrices para garantizar que la información reservada de la Alcaldía Municipal de Floridablanca, sea almacenada, transmitida y recibida de manera segura cumpliendo con la preservación de la confidencialidad e integridad de la misma.

La Dirección de Gobierno Digital debe proporcionar los mecanismos o herramientas necesarias para asegurar la protección de claves de acceso a la red de datos, los sistemas de información y servicios de la Administración Municipal.

- La Dirección de Gobierno Digital debe definir e implementar estándares para la aplicación de controles criptográficos.

- Los dispositivos móviles que manejen información pública reservada o información pública clasificada deberán contar con un sistema de cifrado para prevenir la afectación de esta información.

- Todo sistema de información o servicio tecnológico debe incluir parámetros de seguridad basado en usuarios, perfiles y roles, para ser aplicados en la autorización y autenticación según corresponda.

**Política de transferencia de información**

Garantizar que la información de la Alcaldía Municipal de Floridablanca sea transferida terceros o las personas que la requieran cumpliendo una serie de acuerdos y lineamientos.

- Los controles de seguridad para la transferencia de información se deben seleccionar para mitigar los riesgos de pérdida de confidencialidad, integridad o disponibilidad de la información.

- Los Servidores públicos y contratistas deben seguir las indicaciones del procedimiento de clasificación, etiquetado y manejo de la información de la Administración Municipal de Floridablanca, para la transferencia de información de acuerdo con la clasificación de la misma.

- Los funcionarios públicos de la Administración Municipal que envíen todo tipo de documentación a entidades externas, se debe verificar previamente el envío, el nombre de los destinatarios de la información clasificada como pública reservada,

con el fin de reducir la posibilidad de envío de este tipo de datos, a destinatarios no deseados.

- La Dirección de Gobierno Digital debe implementar las herramientas necesarias para asegurar la transferencia de información al interior y exterior de La Administración Municipal de Floridablanca, contra interceptación, copiado, modificación, enrutador y destrucción.

- En la Alcaldía Municipal de Floridablanca la correspondencia virtual se maneja mediante el correo institucional de cada dependencia de la Administración Municipal de Floridablanca.

- Existen software o aplicaciones que designan las Contralorías o Procuradurías para la transferencia de la información de diferentes dependencias de la Administración Municipal de Floridablanca donde se asignan un usuario y contraseña permitiendo enviar todo tipo de informes y documentos de manera más eficiente y segura.

- La correspondencia que ingresa a la Alcaldía Municipal de Floridablanca, llega a la oficina de gestión documental y se maneja un consecutivo.

## PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

### Procedimiento borrado seguro

La Dirección de Gobierno Digital es la única dependencia encargada de aplicar y realizar el procedimiento de borrado seguro de la información a los medios tecnológicos (impresoras, teléfonos y equipos de cómputo), solo cuando el funcionario se retira de la alcaldía municipal de Floridablanca, se traslada de dependencia o se realiza una modernización del medio tecnológico.

- El funcionario que cumpla con las siguientes causales de borrado seguro ( se retira de la alcaldía municipal de Floridablanca, se traslada de la dependencia o se realiza

modernización del medio tecnológico) realiza la respectiva solicitud llamando a la Dirección de Gobierno Digital

- El técnico/ ingeniero de la Dirección de Gobierno Digital, genera el ticket de la solicitud y le indica al usuario que debe hacer llegar el medio tecnológico a la oficina TIC.

- El técnico/ingeniero recibe el medio tecnológico, verifica el estado del mismo y el usuario firma una autorización de formateo del equipo.

- Se realiza la copia de seguridad de la información del equipo de cómputo teniendo en cuenta lo siguiente:

a. traslado o retiro de la entidad: El usuario debe realizar la copia de seguridad de la información y ser entregada a la oficina de control interno, teniendo en cuenta el reglamento de la alcaldía municipal de Floridablanca, si el usuario no realiza la copia de seguridad la oficina de control interno puede realizar la solicitud al técnico / ingeniero para realizar la copia de seguridad antes de realizar el borrado seguro.

b. Modernización de equipo de cómputo: El usuario realiza la copia de seguridad de la información y lo puede almacenar en el drive del correo institucional o en una unidad de almacenamiento externo provisional que le suministra el técnico/ingeniero.

- El técnico/ ingeniero realiza el formateo, eliminación de usuario y borrado seguro del medio tecnológico.

- Dependiendo de la dependencia donde se encuentra el medio tecnológico, se realiza la asignación del mismo a algún funcionario por orden del jefe o secretario de la dependencia.

- Si el jefe o secretario de la dependencia no desea realizar la asignación del medio tecnológico, este puede realizar la entrega a la oficina de almacén general.

**Procedimiento para el uso de programas utilitarios privilegiados**

Establecer los procedimientos para el uso de programas utilitarios privilegiados de la Alcaldía Municipal de Floridablanca, con la capacidad de anular los controles de sistemas y de aplicaciones.

- La Dirección de Gobierno Digital realiza la instalación de los programas utilitarios necesarios para el funcionamiento del equipo de cómputo al momento de entregar un equipo de cómputo.

- La Dirección de Gobierno Digital debe revisar semestralmente las directrices para el uso de programas utilitarios con la capacidad de anular los controles de sistemas y de aplicaciones.

- la Dirección de Gobierno Digital debe utilizar procedimientos de identificación, autenticación y autorización para los programas utilitarios que requieran los funcionarios para realizar trabajos específicos, así mismo, se llevará un control de los programas utilitarios instalados.

- La Dirección de Gobierno Digital es la única autorizada para instalar, eliminar o modificar los programas utilitarios, si el funcionario instala algún programa de este tipo será eliminado.

- El funcionario que requiera la utilización de un programa utilitario deberá hacer la solicitud al jefe de la Dirección de Gobierno Digital, enviando la información al correo institucionalSistemas@floridablanca.gov.co, Gobiernodigital@floridablanca.gov.co, donde se realizará la viabilidad del programa.

**Procedimiento propiedad intelectual, uso legal de software y productos informáticos.**

Dar cumplimiento a los requisitos contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. Con fin de tener

un mayor control y seguimiento de los programas y/o aplicaciones que reposan en cada equipo o servidor de la Alcaldía de Floridablanca.

- Si se encuentra software ilegal o no cuenta con una licencia válida, se procede a la desinstalación del mismo mediante los procedimientos que realiza la Dirección de Gobierno Digital de la Alcaldía Municipal de Floridablanca.

- Los Software que se adquieren en la Administración Municipal de Floridablanca cuentan con licencias ilimitadas y no incumple con los derechos de propiedad intelectual.

- La Alcaldía Municipal de Floridablanca posee el inventario correspondiente y el software de verificación y control.

**Procedimiento para la transferencia de medios físicos**

Definir acciones que prevengan y eviten la divulgación, modificación, retiro o la destrucción no autorizada de la información almacenada en los medios suministrados por la Alcaldía municipal, cuidando por la disponibilidad y confidencialidad de la información.

- Mantener con las medidas de protección físicas y lógicas de los medios y equipos que permitan su monitoreo y correcto estado de funcionamiento, realizando los mantenimientos preventivos y correctivos que se requieran.

- Los sistemas de información, aplicaciones (software), el servicio de acceso a Internet, Intranet, medios de almacenamiento, cuentas de red, navegadores y equipos de cómputo que son propiedad de la Alcaldía, los cuales deben ser usados únicamente para el cumplimiento misional de la entidad.

- Realizar el procedimiento de borrado seguro en los equipos de cómputo y demás dispositivos, una vez el funcionario haya sido retirado de la Alcaldía.

- Restringir la copia de archivos en medios removibles de almacenamiento, deshabilitando la opción de escritura en dispositivos USB, unidades ópticas de grabación en los equipos de cómputo de la entidad. La autorización de uso de los medios removibles debe ser gestionada a través de la Dirección de Gobierno Digital y será objeto de auditorías de seguridad, apoyado en la prevención de pérdida de información de la Alcaldía.

- El intercambio de información de la Alcaldía con otras organizaciones o terceros debe estar controlado y se debe cumplir la legislación y normas vigentes que correspondan para mantener una adecuada protección de la información la Alcaldía, estableciendo acciones, procedimientos y controles de intercambio de información a través de medios físicos disponibles.

**Lineamiento de seguridad de la información en el ciclo de vida de proyectos**

Integrar diferentes métodos de gestión de proyectos en la Alcaldía municipal de Floridablanca, para asegurar que los riesgos de seguridad de la información que se identifican y se tratan como parte de los diferentes proyectos desarrollados.

- Alinear los objetivos de los proyectos con los de seguridad y privacidad de la información de la entidad.

- Establecer y fijar responsabilidades en roles específicos para gestionar la seguridad de información en los proyectos, de acuerdo con los métodos definidos en la gestión de proyectos.

- Realizar la valoración de riesgos de seguridad en etapas iniciales de los proyectos desarrollados en los diferentes procesos de la alcaldía municipal de Floridablanca, con el propósito de identificar los controles necesarios para mitigar los riesgos.

**Procedimiento para el acceso de áreas de despacho y carga**

Describir los accesos de áreas de despacho y de carga donde los funcionarios, contratistas y visitantes deben ingresar a las instalaciones de la Administración

Municipal de Floridablanca y asegurar solamente el ingreso de personal o visitantes autorizados a las diferentes dependencias al igual que en las áreas catalogadas como seguras.

- El acceso a las zonas de despacho y carga de la Alcaldía de Floridablanca debe ser autorizado por la Administración del edificio o por solicitud directa del funcionario y/o jefe a cargo del área.

- Definir que el área de despacho y carga se debe diseñar de manera que los suministros se puedan cargar y descargar sin que el personal de despacho tenga acceso a otras partes de la edificación.

- Establecer que las puertas externas del área de despacho y carga se aseguran cuando las puertas internas están abiertas.

- Establecer que el material que ingresa se registra de acuerdo con los procedimientos de gestión de activos al entrar al sitio.

- Definir que los despachos entrantes y salientes están separados físicamente, en donde sea posible.

- Todo vehículo que ingrese a dejar o retirar elementos de la Entidad debe estar previamente autorizado por el personal encargado de dicha área.

- La salida de bienes que sean propiedad de la Administración Municipal de Floridablanca deben ser previamente autorizados, por el Jefe del Área a través de correo electrónico enviado por el nivel directivo del área donde pertenecen.

**Procedimiento para la restricción de instalación de software**

Definir las directrices para las restricciones sobre la instalación se software de la Administración Municipal de Floridablanca.

- Cuando algún funcionario de la Alcaldía Municipal de Floridablanca realice un requerimiento para la instalación de un Software, la Dirección de Gobierno Digital está en la obligación de evaluar la necesidad de adquisición de dicho software.

- Todo software que sea instalado en algún equipo de algún funcionario de la Administración Municipal de Floridablanca, debe ser licenciado y aprobado por la Dirección de Gobierno Digital.

- Cuando se realice la instalación de un software se deben tener en cuenta las características y/o capacidades de los equipos de cómputo.

- La Dirección de Gobierno Digital debe tener un inventario del software licenciados e instalados en la Administración Municipal de Floridablanca

- Ningún software licenciado de la Alcaldía Municipal de Floridablanca, bajo ninguna circunstancia debe proporcionarse a personas u organizaciones externas o usarse con fines de lucro.

**Procedimiento para trabajo en áreas seguras**

Definir los lineamientos para el trabajo en áreas seguras en las instalaciones y sedes de la Alcaldía Municipal de Floridablanca.

La Alcaldía Municipal de Floridablanca debe mantener áreas seguras de trabajo para la gestión, almacenamiento y procesamiento de la información en la Entidad. Teniendo en cuenta lo postulado con anterioridad, se definieron los siguientes lineamientos:

- Se deben definir perímetros de seguridad según las necesidades del área de trabajo y perfiles de los empleados que estén involucrados.

- La entidad debe designar y aplicar protección física para la prevención de desastres como: incendios, inundaciones, terremotos, explosiones, manifestaciones y otras formas de desastre natural o humano.

- Para áreas con centros de cómputo y/o cableado se debe velar por el ambiente adecuado para los activos informáticos, controlando temas de ventilación, iluminación, regulación de corriente, entre otros.

- Se debe tener un control de acceso físico a zonas que lo requieran, como pueden ser centros de bodegaje de archivos, activos físicos de sistemas de información, centros de datos, entre otros.

- Cuando un área que maneje información crítica de la Administración Municipal esté vacía o no se encuentre personal trabajando en estas áreas, se deberá mantener la zona con los recursos de seguridad correspondientes, como pueden ser, puertas cerradas con llave, bloqueos con único acceso a través de medios biométricos, cámaras activas y sensores de movimiento (alarmas) según se requiera.

- El uso de dispositivos de grabación y/o registro fotográfico tales como cámaras en dispositivos móviles están restringido en las áreas seguras de trabajo de la Administración Municipal, a menos que se cuente con una autorización para ello.

- Se debe evitar el trabajo no supervisado en las áreas seguras de la Administración Municipal, con el fin de proteger la integridad y seguridad de la información que se maneje en dicha área.

- La responsabilidad del ingreso a áreas denominadas como seguras será exclusiva del responsable de dicha área.

- Se deben usar los elementos de protección personal que el área segura requiera.

**CUMPLIMIENTO**

Todos los secretarios, directores, funcionarios y contratistas de la alcaldía municipal de Floridablanca, debe cumplir con el 100% de la política.

## REVISIÓN Y ACTUALIZACIÓN DE LA POLÍTICA

La Dirección de Gobierno Digital actualizará la política general de seguridad de la información, políticas de seguridad de la información y los procedimientos de seguridad de la información, una vez al año con la aprobación de la alta dirección, teniendo en cuenta el monitoreo de los procesos y controles.

## PROCEDIMIENTO PARA REPORTAR INCIDENTES DE SEGURIDAD

**Objetivo:**

Gestionar de manera adecuada los eventos, incidentes y vulnerabilidades de seguridad de la información que se generen en la alcaldía municipal de Floridablanca con el fin de prevenir y limitar el impacto de los mismos.

**Aplicabilidad:**

La política de procedimiento para reportar incidentes de seguridad aplica a la alta dirección, secretarios, jefes, funcionarios y contratistas de la Alcaldía Municipal de Floridablanca.

**Detalle:**

Cualquier incidente de seguridad de información que se presente en la Alcaldía Municipal de Floridablanca se debe reportar de manera oportuna a la Dirección de Gobierno Digital para tomar las medidas pertinentes frente al caso.

- Se deben recolectar las evidencias y documentar todos los incidentes de seguridad de la información.

- Se debe llevar un registro de todos los incidentes, vulnerabilidades y eventos reportados y su respectiva solución.

- Dependiendo del incidente de seguridad de la información que se esté tratando, la Dirección de Gobierno Digital es la única autorizada para contactar con las entidades de control pertinentes, descritas a continuación:

| **Nombre de la Entidad** | **Contacto** | **Detalle** | **Cómo reportar un Incidente** |
|---|---|---|---|
| | | El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - | Para reportar un incidente o vulnerabilidad deberá escribir directamente a: |

**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:**

La entidad deberá documentar una política general de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Debe ir dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información.

La política debe contemplar para su elaboración los siguientes parámetros:

- Debe estar aprobada por la alta dirección, certificando así el compromiso con el proceso.
- **Visión General:** ¿Qué se debe reportar? ¿A quién debe reportarse?, ¿Qué medios pueden emplearse para hacer el reporte?

- **Definir Responsables:** Se deben mencionar de manera muy general quienes serán los responsables de gestionar los eventos.
- **Actividades:** Explicar de manera general en que consiste el proceso de gestión de incidentes desde el reporte hasta la resolución.
- **Documentación:** Se debe hacer referencia sobre la documentación del esquema de gestión y los procedimientos.
- **Descripción Del Equipo Que Manejará Los Incidentes:** Se debe indicar como está compuesta la estructura general para la gestión de incidentes y vulnerabilidades de seguridad.
- **Aspectos Legales:** Deben citarse los aspectos legales que se deben tener en cuenta o los cuales debe darse cumplimiento.

## CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Esta política se centra en la formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

Dicha política debe contener los siguientes parámetros.

- El compromiso de la alta dirección en destinar los recursos suficientes para desarrollar los programas.
- ¿Quiénes deberán ser entrenados? ¿Quiénes deberán ser sensibilizados?
- La obligación de los usuarios a asistir a los eventos o cursos de capacitación
- Revisión periódica de resultados de capacitaciones para mejoramiento de los procesos.
- Definir los roles y responsabilidades de quienes diseñarán los programas, quienes los comunicarán.
- Documentación sobre planes de estudio y desarrollo de los programas.
- Compromisos y obligaciones por parte del personal capacitado.
- Contener políticas adicionales relacionadas directamente con el debido comportamiento de los usuarios usuarios como las siguientes:
  - Política De Escritorio Limpio
  - Política De Uso Aceptable
  - Ética Empresarial.