PROTOCOLO DE POLÍTICAS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN – S.G.S.I.

MARTÍN EMILIO SÁNCHEZ VALENCIA
Alcalde Municipal 2020 - 2023

Aprobado por el Comité Institucional de Gestión y Desempeño

QUIBDÒ
2020

CONTENIDO

INTRODUCCIÒN

En la Alcaldía Municipal de Quibdó, reconoce que la información es un componente indispensable para la prestación de sus servicios y la toma de decisiones, por esta razón es necesario definir y establecer una guía de seguridad de la información que proteja de manera apropiada los datos. Este documento da a conocer a fondo las políticas y normas de seguridad de la información definidas por la Alcaldía, el cual se toma como base fundamental la norma ISO 27001: 2013.

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

La seguridad de la información es importante y prioritaria para la Alcaldía Municipal de Quibdó, se debe asumir con responsabilidad por todo el personal de la alcaldía, además estas políticas se cumplan de manera adecuada y que no incumpla o contradiga lo estipulado en este documento.

La Alcaldía Municipal de Quibdó, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la administración de riesgos y la consolidación de una cultura de seguridad.

OBJETIVOS:

OBJETIVO GENERAL:

- Definir en la Alcaldía de Quibdó la política de seguridad de la información para aprovechar al máximo la información que maneja cada funcionario público y emitir herramientas para mitigar los riesgos identificados en el campo de la seguridad de la información.

OBJETIVOS ESPECÍFICOS:

- Lograr que todas y cada una de las oficinas y dependencias adscritas a la Alcaldía Municipal de Quibdó – Chocó, se acojan al protocolo del Sistema de Gestión de Seguridad de la Información.

- Mantener los protocolos de seguridad en documentos físicos y electrónicos de la Alcaldía Municipal de Quibdó – Chocó.

ALCANCE

Con el fin de lograr un adecuado nivel de protección en la seguridad de la información de la Administración Municipal, las políticas de seguridad aplican para todos los usuarios internos y externos, de la Alcaldía Municipal de Quibdó, por lo cual se quiere que dicha seguridad en la información se extienda a la información tanto en físico como en electrónico al interior de la entidad.

1. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Los riesgos en la seguridad de la información de la Administración Municipal se pueden clasificar: Actos originados por la criminalidad común, Riesgos por sucesos de origen físico y riesgos por sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales:

1.1 ACTOS ORIGINADOS POR LA CRIMINALIDAD COMÚN

- Sabotaje (ataque físico y electrónico).
- Daños por vandalismo.
- Fraude / Estafa.
- Robo / Hurto (físico).
- Robo / Hurto de información electrónica.
- Virus.
- Ejecución no autorizado de programas.
- Violación a derechos de autor.

1.2 RIESGOS POR SUCESOS DE ORIGEN FÍSICO

- Incendio.
- Inundación.
- Sismo.
- Polvo.
- Falta de ventilación.
- Sobrecarga eléctrica.
- Falla de corriente (apagones).
- Falla de sistema / Daño disco duro.

1.3 NEGLIGENCIA DE USUARIOS Y DECISIONES INSTITUCIONALES

- Falta de inducción, capacitación y sensibilización sobre riesgos.
- Mal manejo de sistemas y herramientas.
- Utilización de programas no autorizados / software ilegal.
- Falta de pruebas de software nuevo con datos productivos.
- Perdida de datos.
- Infección de sistemas a través de unidades portables sin escaneo.
- Manejo inadecuado de datos críticos (codificar, borrar, etc.).
- Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas).
- Compartir contraseñas o permisos a terceros no autorizados.
- Transmisión de contraseñas por teléfono.
- Acceso electrónico no autorizado a sistemas externo.

2. POLÍTICAS, CONTROLES, RECOMENDACIONES Y OPERACIONES BASICAS

2.1 COMPUTADORES, PORTATILES, SERVIDORES

2.1.1 Políticas. Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la Alcaldía Municipal de Quibdó sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones.

2.1.2 Controles:

- ✓ El equipo de cómputo será asignado de acuerdo al puesto o función laboral en su área de trabajo. Siendo el responsable de dicha asignación el Jefe de cada dependencia.
- ✓ Cada equipo está preparado con el Hardware y Software básico necesario para su funcionamiento, el usuario no deberá alterar el contenido físico y/o lógico del mismo incluyendo sus periféricos.
- ✓ En caso de presentar una falla física o lógica se deberá notificar al área de sistemas y en el caso de ser requerido enviar el equipo para su revisión y/o reparación de acuerdo al procedimiento establecido
.
- ✓ En ningún caso el usuario intentará reparar el equipo ó diagnosticarlo, únicamente debe informar de la posible falla.
- ✓ El usuario será el único responsable del equipo de cómputo.
- ✓ En ningún caso, el usuario tendrá cerca alimentos, bebidas u otros materiales que puedan derramarse sobre el equipo.
- ✓ Solo se utilizará el equipo para funciones de interés del área y de ninguna manera para asuntos personales.
- ✓ El personal asignado deberá comprobar sus conocimientos o experiencia en el manejo del equipo de cómputo y periféricos básicos.
- ✓ En caso de que el usuario no tenga conocimientos y/o experiencia, se notificará al área de sistemas para su correspondiente Capacitación.

- ✓ La adquisición de equipo será con cargo al presupuesto de cada área o de la secretaria general, las características técnicas serán proporcionadas por el área de sistemas.

- ✓ La solicitud del equipo de cómputo será responsabilidad del área interesada, bajo las características técnicas definidas por el área de sistemas e informando a las áreas relacionadas con la asignación de los recursos.

- ✓ Toda recepción de equipo de cómputo por adquisición o donación se realizará a través del Área de Inventarios, con el apoyo del área de sistemas.

- ✓ La salida de equipo de cómputo del Almacén, será total responsabilidad del almacén, el cual revisará la integridad física y el área de sistemas instalará la integridad lógica e instalará y preparará el software y hardware correspondiente a las licencias contenidas.

- ✓ Cada equipo contiene el software de acuerdo a las necesidades del área de trabajo, El cual No deberá ser alterado.

- ✓ Por ningún motivo el usuario instalará software de promoción y/o entretenimiento.

- ✓ La adquisición o desarrollo de software será responsabilidad del área de sistemas.

- ✓ El usuario deberá reportar de forma inmediata al Área de Sistemas cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, contactos eléctricos con riesgo de incendio u otros.

- ✓ El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

- ✓ Es responsabilidad del usuario evitar en todo momento la fuga de la información de la institución que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

- ✓ Cualquier persona que tenga acceso a las instalaciones de la alcaldía, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

- ✓ Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrán salir de las instalaciones únicamente con la autorización de salida del área de Inventarios anexando el vale de salida del equipo debidamente por el secretario de la oficina o la equivalente en las dependencias de la institución.

- ✓ Los centros de cómputo u oficina de servidores de la Institución son áreas restringidas, por lo que sólo el personal autorizado por el área Sistemas puede acceder a ellos.

- ✓ Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Área de Sistemas, en caso de requerir este servicio deberá solicitarlo a través de la mesa de ayuda.

- ✓ El Área de Inventarios será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el área de Sistemas.

- ✓ El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de la alcaldía.

- ✓ Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

- ✓ Es responsabilidad de los usuarios almacenar su información únicamente en la partición de disco duro en el servidor o equipo, o en su defecto en la carpeta “Mis Documentos” ya que las otras están destinadas para archivos de programa y sistema operativo.

- ✓ Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del computador.

- ✓ Se debe mantener el equipo informático en un entorno limpio y sin humedad.

- ✓ Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación al área de Sistemas a través de un plan detallado o una solicitud para el debido acompañamiento del área de sistemas.

- ✓ Queda prohibido que el usuario abra o desarme los equipos de cómputo.
- ✓ Únicamente el personal autorizado por el Área de Sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático.
- ✓ El usuario deberá dar aviso inmediato al Área de Sistemas e Inventarios de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.
- ✓ El uso de los grabadores de discos externos es exclusivo para copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.
- ✓ El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se les dé.
- ✓ El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, se levantara un reporte de incumplimiento de políticas de seguridad.
- ✓ Los equipos de la Alcaldía sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
- ✓ Debe respetarse y no modificar la configuración de hardware y software establecida por el Área de sistemas.
- ✓ Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el bloqueo de pantalla para que se active al cabo de 20 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además, el usuario debe activarlo manualmente cada vez que se ausente de su oficina.
- ✓ Si un computador tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.
- ✓ Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en computadores que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Alcaldía.
- ✓ A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

- ✓ Los usuarios no deben copiar a un medio removible (como una USB), el software o los datos históricos residentes en las computadoras de la Alcaldía, sin la aprobación previa del área de sistemas o del jefe inmediato.

- ✓ No pueden extraerse datos fuera de la institución sin la aprobación previa de la Administración. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como Internet.

- ✓ Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al área de sistemas y poner el computador en cuarentena hasta que el problema sea resuelto.

- ✓ Sólo pueden descargarse archivos de redes externas de acuerdo a los procedimientos establecidos.

- ✓ Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otras dependencias de la institución.

- ✓ No debe utilizarse software descargado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el área de sistemas.

- ✓ Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el área de sistemas.

- ✓ Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

- ✓ No deben usarse USB u otros medios de almacenamiento en cualquier computador de la institución a menos que se haya sido previamente verificado que están libres de virus u otros agentes dañinos.

- ✓ Periódicamente debe hacerse el respaldo de los datos guardados en computadores y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de la institución deben guardarse en otra sede, lejos del edificio.

- ✓ Los usuarios de computadores son responsables de proteger los programas y datos contra pérdida o daño.

- ✓ El área de sistemas será responsable de la generación de las copias de seguridad de los equipos de la entidad y definirá la frecuencia del respaldo.

- ✓ Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante de la alcaldía.

- ✓ No debe dejarse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la alcaldía.

- ✓ El personal que utiliza un computador portátil que contenga información confidencial de la alcaldía, no debe dejarlo desatendido, sobre todo cuando esté de viaje.

- ✓ Todos los equipos permanecerán en el lugar registrado por el área de almacén.

- ✓ Solo los equipos portátiles de propiedad de la Alcaldía Municipal de Quibdó podrán desplazarse con previa autorización del responsable de la dependencia y bajo la responsabilidad total del usuario.

3. USO DE INTERNET

3.1 POLÍTICAS

La Alcaldía Municipal de Quibdó es consciente de la importancia de Internet como herramienta para el desempeño de las tareas, y proporcionará los recursos necesarios para que los usuarios que necesitan Internet para sus actividades diarias puedan utilizarlo.

3.2 CONTROLES

- ✓ El acceso a internet deberá encontrarse protegido por filtros para disminuir sitios peligrosos que contengan códigos maliciosos o que se encuentren ajenos al servicio, Permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus.
- ✓ No navegar por sitios no confiables.
- ✓ Se prohíbe el uso de sitios de radios online a excepción de sitios institucionales.
- ✓ Se prohíbe el uso de intercambio de archivos a través de sistemas o programas de internet, sin que estos cuenten con la debida acreditación y controles de seguridad.
- ✓ Se prohíbe el uso de sitios de chat (Messenger, chat, etc.), a menos que este sea de uso institucional.
- ✓ Se prohíbe el uso de internet para actividades ilícitas.
- ✓ Se prohíbe la descarga que no cumpla con la normativa vigente de copyright y similar.
- ✓ Se prohíbe el acceso a los sitios o páginas Web que contengan materiales amenazadores, pornográficos, racistas, sexistas o cualquier otro que degrade la calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.
- ✓ No compartir sus claves para ingresar a sitios que lo requiera (Bancos, Correo).
- ✓ No permitir que el navegador de internet recuerde la contraseña automáticamente.
- ✓ Evitar participar en juegos de entretenimiento en línea.
- ✓ Si no está navegando por internet, cierre todas las ventanas abiertas.

- ✓ Cualquier archivo que se reciba o descargue de internet deberá revisarse con el antivirus para asegurar que no tenga virus.
- ✓ Si requiere navegar en algún sitio bloqueado se deberá solicitar al área de sistemas.

4. MANEJO DE REDES SOCIALES

4.1 POLÍTICAS

La Alcaldía Municipal de Quibdó define pautas generales para asegurar que los usuarios autorizados puedan proteger adecuadamente la información y manejarla de manera adecuada cuando utilicen las redes sociales.

4.2 CONTROLES

- ✓ En lo posible la alcaldía deberá bloquear todo tipo de sitio relacionado con redes sociales, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus. Si algún funcionario por motivos de trabajo requiera acceder a ellos, deberá enviar la solicitud formal al área de sistemas.

- ✓ Solo podrán tener acceso a redes sociales un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.

- ✓ La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la alcaldía municipal, que sea creado a nombre personal, como redes sociales, twitter, facebook, youtube o blogs, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

5. MANEJO DE IMPRESORAS

5.1 POLÍTICAS

Estas políticas son necesarias con el fin de asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

5.2 CONTROLES

- ✓ Los documentos que se impriman en las impresoras de la alcaldía municipal deben ser de carácter institucional.
- ✓ Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.
- ✓ Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar a la alcaldía municipal.

6. MANEJO APROPIADO DE CONTROL DE VIRUS

6.1 POLÍTICAS

La Alcaldía Municipal de Quibdó con el fin de definir lineamientos generales que aseguren la adecuada protección de la información y el manejo adecuado de los equipos, la Alcaldía ha desarrollado lineamientos a seguir para proteger los activos de la entidad frente a amenazas informáticas.

6.2 CONTROLES

- ✓ La alcaldía deberá definir un producto estándar licenciado entorno de sus estaciones de trabajo, resguardando el correcto funcionamiento de los equipos computo.
- ✓ El sistema de actualizaciones y detección diaria deberá estar automatizado.
- ✓ Se debe comunicar de cualquier infección por virus que no fue eliminada por el antivirus, al área de sistemas.
- ✓ Los usuarios no podrán desinstalar o cambiar el producto de antivirus existente en su equipo.
- ✓ Los dispositivos extraíbles, antes de ser usados deben ser escaneados con el antivirus.

7. SWITCHES Y ROUTERS

7.1 POLÍTICA

El área de sistemas es absolutamente responsable de la gestión de los equipos de red, los routers y switches a disposición de la alcaldía para garantizar que estén dispuestos física y lógicamente en un lugar seguro y protegido.

7.2 CONTROLES

- ✓ Las contraseñas predefinidas que traen los dispositivos nuevos, deben cambiarse inmediatamente al ponerse en servicio el dispositivo.
- ✓ Se deberá designar al personal que efectuará las actividades de instalación, desinstalación, mantenimiento y conexión física de estos dispositivos.
- ✓ Definir procedimientos de recuperación ante eventualidades físicas.
- ✓ Definir procedimientos de respuesta, autoridades y los objetivos de la respuesta después de un ataque exitoso, incluir esquemas de preservación de la evidencia.
- ✓ Se deberán enumerar protocolos, puertos y servicios a ser permitidos o filtrados en cada interface, así como los procedimientos para su autorización.
- ✓ Se deberán identificar los servicios de configuración dinámica de los Routers, y las redes permitidas para acceder a dichos servicios.
- ✓ Se deben tener plenamente identificados los protocolos de ruteo a utilizar, y los esquemas de seguridad que proveen Seguridad en el Router.

8. CORREO ELECTRÓNICO INSTITUCIONAL

8.1 POLÍTICA

El correo electrónico es personal e intransferible. Cada usuario es responsable de mantener el uso de este contenido y su contraseña bajo estas dos premisas, y no debe permitir que nadie fuera del alcance de su dependencia acceda a este recurso por ningún motivo. . Todos estos han facilitado la comunicación entre funcionarios y terceros. Por lo tanto, la Alcaldía brindará servicios ideales y seguros para la realización de actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de las personas que se comunican por este medio.

8.2 CONTROLES

- ✓ Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de la Alcaldía Municipal.
- ✓ Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- ✓ El Correo electrónico institucional es de uso exclusivo para actividades relacionadas con la alcaldía y queda restringido el uso para otros fines.
- ✓ Se prohíbe expresamente el envío de archivos, transmisión o almacenamiento de cualquier información que pudiera ser considerada pornográfica, difamatoria, racista, música, videos, etc., o que atente contra las buenas costumbres o principios.
- ✓ La contraseña de correo debe ser cambiada periódicamente e informar de la nueva contraseña al área de sistemas.
- ✓ No abrir link sospechoso llegados por correos electrónicos (bancos, tiendas, etc.).
- ✓ No completar datos personales en correos electrónicos sospechosos.
- ✓ Eliminar periódicamente los correos no deseados (spam o sospechoso).
- ✓ Los Accesos a la red (Internet) serán solo de interés laboral y no personal.

- ✓ De ninguna manera se podrá acceder a páginas de entretenimiento, pornografía o fuera del contexto laboral.
- ✓ El usuario no deberá bajar (ó copiar) archivos sospechoso o con extensiones desconocidas de la red sin autorización del área de sistemas.
- ✓ La comunicación estará limitada por las políticas de seguridad del área de sistemas.
- ✓ Solo se enviará y recibirá información de interés laboral.
- ✓ En ningún caso de recibir información en archivos adjuntos de dudosa procedencia o que no esté esperando, se notificará al área de sistemas, para analizar y evitar que ingresen virus al sistema.
- ✓ Al enviar información el responsable será el usuario correspondiente.
- ✓ No se deberá enviar información de tipo estadístico, informativo o información relevante de las acciones de la Dirección, Área de trabajo o del Gobierno Municipal a ningún destino no autorizado.
- ✓ El uso de Internet está limitado por las políticas de seguridad del área de sistemas.

9. BASES DE DATOS

9.1 POLÍTICA

La Alcaldía Municipal, especialmente los administradores de bases de datos, están obligadas a controlar todo tipo de gestión que se realice sobre la base de datos y a velar por que esté protegida de diversos tipos de ataques, destrucción o intrusión, ya sean internos o externos, y en este caso, debe tomar acciones correctivas necesarias para restaurar su funcionamiento sin pérdida de información.

Es política de la institución prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su política proteger la información que pertenece a otras empresas o personas y que le haya sido confiada.

9.2 CONTROLES

- ✓ Es función del administrador especificar los privilegios que un usuario tiene sobre la base de datos La base de datos debe estar protegida contra el fuego, el robo y otras formas de destrucción.
- ✓ Se debe garantizar que los datos sean reconstruidos en caso de daño, efectuando periódicamente un respaldo de la información.
- ✓ Los datos deben poder ser sometidos a procesos de auditoria. La falta de auditoria en los sistemas de computación ha permitido la comisión de grandes delitos.
- ✓ El sistema debe tener capacidad para verificar que sus acciones han sido autorizadas. Las acciones de los usuarios deben ser supervisadas, de modo tal que pueda descubrirse cualquier acción indebida o errónea.
- ✓ Se deberá demorar la respuesta de la base de datos ante claves erróneas aumentando la demora cada vez y se alertará si hay demasiados intentos.
- ✓ Registrar todas las entradas cada vez que un usuario entra, se debe chequear cuándo y desde dónde entró la vez anterior.
- ✓ Hacer chequeos periódicos de claves fáciles de adivinar, procesos que llevan demasiado tiempo corriendo, permisos erróneos, actividades extrañas (por ejemplo, cuando usuario está de vacaciones).

- ✓ Se deberá contar con un sistema de manejo de autorizaciones con el fin de usar derechos de acceso dados por el terminal, por la operación que puede realizar o por la hora del día.

- ✓ Uso de técnicas de cifrado para proteger datos en la base de datos.

- ✓ Manejo de la tabla de usuarios con código y contraseña, control de las operaciones efectuadas en cada sesión de trabajo por cada usuario y anotadas en la bitácora, lo cual facilita la auditoría de las bases de datos.

10. RED LAN

10.1 POLÍTICA

Las actividades que no estén autorizadas por el dominio del sistema, en las que los usuarios exploren los recursos informáticos en la red de la organización y las actividades de las aplicaciones antes mencionadas, serán consideradas como ataques de seguridad y delitos graves.

Por este motivo la alcaldía municipal como responsables de las redes de datos y los recursos de red de la alcaldía, debe propender porque dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

10.2 CONTROLES

- ✓ El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reacomodo de cables con el personal de Sistemas.
- ✓ La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y del Área de Sistemas.
- ✓ Todos los cambios en la central telefónica y en los servidores y equipos de red de la alcaldía, incluyendo la instalación del nuevo software, el cambio de direcciones IP, la reconfiguración de Routers y Switches, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.
- ✓ El acceso a Internet provisto a los usuarios de la alcaldía es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.
- ✓ La solicitud para la conexión de nuevos equipos a la red de la alcaldía deber hacerse a través desde un correo institucional, por ningún motivo se permitirá la conexión de nuevos equipos sin la previa autorización del área de sistemas.

- ✓ Solo se pueden conectar a la red los dispositivos móviles que cuenten con la aprobación del área de sistemas, para lo cual debe justificar el motivo por el cual debe conectar este a la red de la alcaldía municipal.

- ✓ En caso de necesitar una conexión a Internet especial, ésta tiene que ser notificada y aprobada por el Área de Sistemas.

- ✓ Los usuarios de Internet de la Alcaldía tienen que reportar todos los incidentes de seguridad informática al Área de Sistemas inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

- ✓ Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que: serán sujetos de monitoreo de las actividades que realiza en Internet, ya que saben que existe la prohibición al acceso de páginas no autorizadas, saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados, y saben que existe la prohibición de descarga de software sin la autorización del Área de Sistemas.

- ✓ La utilización de Internet es para el desempeño de su función y no para propósitos personales.

- ✓ Los servidores de red y los equipos de comunicación (Routers, switches, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

11. MANEJO DE CUENTAS DE USUARIOS

- ✓ Toda cuenta de acceso que se requiera modificar deberá ser solicitada al área de sistemas.
- ✓ El procedimiento de creación de cuentas, debe ser canalizado a través del área de sistemas.
- ✓ En caso de tener algún problema al acceder a la cuenta de usuario, el funcionario se debe notificar inmediatamente al área de sistemas y no tratar de solucionarlo.
- ✓ El área de sistemas de tener a su disposición todas las contraseñas de los equipos a cargo de la administración municipal de la Alcaldía Municipal de Quibdó.

12. OPERACIONES BÁSICAS DE PC

12.1 POLÍTICA

Para el buen uso y funcionamientos de los pc deber seguirse unos pasos para asegurar su buen funcionamiento:

- ✓ Para encender el sistema de cómputo verifique que el monitor, CPU, impresora y demás periféricos estén debidamente instalados entre si y conectados a la corriente eléctrica.
- ✓ Enseguida identifique los interruptores o botones de encendido y apagado presione o mueva según se requiera.
- ✓ Encienda la impresora, regulador, monitor, y demás periféricos que tenga instalados dejando al final el CPU.
- ✓ Para apagar el sistema presione o mueva los interruptores según se requiera en el mismo orden antes mencionado.

Cuando encender y apagar el Sistema:

- ✓ Al inicio y fin de las actividades.
- ✓ En caso de tormentas eléctricas.
- ✓ Si se presentan fallas eléctricas.

13. CONTRASEÑAS Y EL CONTROL DE ACCESO

13.1 POLÍTICA

Controlar el acceso a la información.

13.2 CONTROLES

- ✓ El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada, así como tampoco usar números telefónicos ni nombres de familiares. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
- ✓ Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.
- ✓ Cambiar la contraseña regularmente e informar del cambio a la oficina de sistemas.
- ✓ Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.
- ✓ Nunca grabar la contraseña en una tecla de función o en un comando de caracteres pre-definido.
- ✓ Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.
- ✓ La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.
- ✓ No utilizar la opción de almacenar contraseñas en Internet.
- ✓ Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

- ✓ Todas las contraseñas para acceso al Sistema Web con carácter administrativo deberán ser cambiadas al menos cada 6 meses.

- ✓ Se evitará el utilizar la misma contraseña para acceso a los sistemas operativos y/o a las bases de datos u otras aplicaciones.

- ✓ Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la alcaldía, pudiendo ser causal de despido.

- ✓ Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

13.3. PARÁMETROS PARA LA CREACIÓN DE UNA CONTRASEÑA:

- ✓ Contraseñas fuertes que contengan números y letras, mayúsculas y minúsculas.

- ✓ Utilizar contraseña que tengan por lo menos 8 caracteres alfanuméricos.

- ✓ Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.

- ✓ No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.

14. CUMPLIMIENTO SEGURIDAD INFORMÁTICA

14.1 POLÍTICA

Funciones del área de sistema de la Alcaldía es recomendar y revisar el cumplimiento de las políticas de seguridad, para asegurar que se tomen las medidas preventivas y correctivas para apoyar los equipos e instalaciones de cómputo, y los bancos de datos de información automatizados.

14.2 CONTROLES

- ✓ Los sistemas desarrollados por personal interno o externo que controle el área de Sistemas son propiedad intelectual de la Alcaldía Municipal.
- ✓ El Área de sistemas podrá implantar mecanismos de control que permitan identificar tendencias en el uso de los recursos informáticos por parte del personal interno o externo. El mal uso de los recursos informáticos que sea detectado debe ser reportado.
- ✓ Esta absolutamente prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el área de sistemas.
- ✓ Ningún empleado de la Alcaldía Municipal de Quibdó puede intentar probar fallas en la seguridad, a menos que estas pruebas sean controladas y aprobadas por el departamento de sistemas.
- ✓ Se prohíbe absolutamente la escritura, generación, compilación, copia, colección, propagación, ejecución o intento de introducir cualquier tipo de código malicioso o potencialmente dañino conocidos como virus, gusanos o caballos de Troya, diseñados con el único fin de auto replicarse para dañar o afectar el desempeño o acceso a los centros de cómputo, redes o información de la Alcaldía Municipal de Quibdó.
- ✓ Los jefes de área o dependencia deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información.

15. PROCEDIMIENTOS O MANEJO DE INCIDENTES ESTÁNDAR PARA TRATAMIENTO DE FALLOS

Entiéndase por Incidente todo aquel evento extraordinario que ocurra con los activos evaluados de la Alcaldía Municipal de Quibdó: por ejemplo, Mantenimiento preventivo de uno o todos los computadores (Anual o Preventivo), Fallo de Activos, etc. El procedimiento en cualquiera de estos casos se debe registrar teniendo en cuenta los siguientes pasos:

En caso de falla de un activo se debe:

1. Enviar un correo electrónico desde el correo institucional de la oficina al correo del área de sistemas, donde especifique:
a) Nombre del usuario
b) dependencia donde labora
c) datos de contacto celular, teléfono o extensión
d) la falla que se vaya a reportar siendo muy claros sobre esta.

2. En caso de no poder enviar el correo debe comunicarse en su defecto al número del área de sistemas para la asignación del personal y del número de caso de este.

3. En caso de no ser factible ninguna de las opciones anteriores También puede acercarse a la oficina de Sistemas donde se tomará el servicio y se asignará el técnico.

Es de vital importancia comunicar los fallos a tiempo ya que de esto depende su pronta resolución.

Para el caso de realizar mantenimiento el preventivo anual:

1. Se debe pasar el cronograma de actividades de los mantenimientos donde se especifique la dependencia sobre la cual se van a realizar, así como la fecha en que estos se van a efectuar. Lo anterior con la previa autorización del jefe o líder del área de sistemas, o el encargado del área al cual pertenezca.

2. Se deben utilizar los formatos pre establecidos para estos procedimientos.

3. En caso de algún cambio en el hardware o software del equipo, este debe ser colocado en la hoja de vida del equipo de cómputo.

16. IMAGEN INSTITUCIONAL

- ✓ Todos los equipos podrán tener como imágenes predeterminadas aquellas que sean institucionales.
- ✓ En el exterior de todos los equipos se respetará la imagen física de empaque.
- ✓ Todos los accesorios de apoyo podrán tener plasmadas imágenes institucionales.
- ✓ Cada usuario es responsable del cuidado de su herramienta de trabajo. Por lo que se recomienda limpiar continuamente el equipo externamente.

17. SEGURIDAD PERSONAL

17.1 RECOMENDACIONES GENERALES

- ✓ Parpadee continuamente para evitar que las pupilas se sequen, especialmente si usa lentes de contacto.
- ✓ Cambie periódicamente la dirección de su mirada para descansar el nervio ocular.
- ✓ Realice constantemente ejercicios de visión periférica.
- ✓ Mantenga limpia la pantalla del monitor para facilitar la lectura y evitar reflejos.
- ✓ Ajuste la brillantez de la pantalla.
- ✓ Ajuste la posición de la pantalla y las fuentes de iluminación (luz natural y eléctrica).
- ✓ Coloque el monitor y los documentos fuente de manera que ambos estén aproximadamente a la misma distancia de sus ojos.
- ✓ Si utiliza lentes que sean con un marco completo para leer a una distancia de 50 a 60 centímetros.

18. POLÍTICAS GENERALES

Los responsables de cada área deberán apoyar al cumplimiento de los lineamientos antes mencionados.

Todo usuario tendrá que cumplir con los lineamientos antes mencionados de lo contrario se hará acreedor a una sanción que se designará por el nivel directivo.

Las medidas anteriores son enunciativas y no limitativas, el área de sistemas se mantendrá en contacto con los usuarios para hacerles saber de las nuevas disposiciones tecnológicas y de procedimientos.

18.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La información es un recurso valioso para la Alcaldía Municipal de Quibdó, la cual apoyada en su misión, visión y objetivos estratégicos expresa su compromiso en la minimización de los riesgos a los cuales está expuesta la información, impulsando una cultura de seguridad, gestionando los incidentes de seguridad, con el fin de garantizar la continuidad de los procesos principales y lograr la mejora continua.

Todos los funcionarios y personal contratista garantizan la protección de la información, a la cual tenga acceso para evitar pérdida, daño o uso no autorizado, el incumplimiento de los controles y política de seguridad será reportada y se realizará seguimiento.

La alcaldía Municipal reconoce que la información suministrada por cada funcionario público es de su propiedad y debe estar custodiada en las instalaciones establecidas por la Administración Municipal. De esta forma se constituye el compromiso por parte de todos los funcionarios públicos del uso adecuado de la información y de los controles que mitigan los riesgos identificados.

18.2 PROPIEDAD DE LA INFORMACIÓN

La información cuya propiedad es de la Alcaldía Municipal es asignada a cada funcionario de acuerdo a sus funciones y actividades laborales para su respectiva custodia, sin que esto anule la propiedad que tiene la Alcaldía sobre los activos de información. Asignar un activo de información a un funcionario público se realiza con el fin de establecer responsabilidades en el uso de la información para conservar su integridad, confidencialidad y disponibilidad.

18.3 RESPONSABILIDAD FRENTE A LA SEGURIDAD

- ✓ La seguridad de información es una obligación y responsabilidad de todos los funcionarios públicos de la Alcaldía de Quibdó sin excepción alguna.

- ✓ La Alcaldía define los roles y responsabilidades frente a la custodia y protección de la información, estableciendo privilegios en los usuarios de dominio en la red para que cada uno sea responsable de acuerdo al grado de confidencialidad protección y privacidad.

- ✓ Periódicamente el encargado de sistemas realizara un sistema de Backups con el fin de almacenar dicha información en Discos y posterior transferencia al archivo central de la Alcaldía Municipal.

19. SEGURIDAD FÍSICA

19.1 DEFINICIÓN

Se definen como acciones de seguridad física todas aquellas que involucran en su componente principal al entorno propio donde se están desarrollando las actividades de una organización, en este caso, las instalaciones de la Alcaldía y aquellas que por razones propias de sus actividades están localizadas fuera de ella, consistiendo en prevenir y mitigar cualquier riesgo y/o amenaza que puedan afectar los recursos que estén dentro de ese entorno.

Los equipos de la Alcaldía cuentan con claves de usuario para que personas ajenas al grupo de trabajo no tengan acceso a ellos, esto se realiza con el objetivo de evitar pérdida y daño de información. En caso de riesgos generados por sucesos físicos se deberán generar copias de seguridad de los backups en por lo menos un lugar diferente a la Alcaldía Municipal y mantener el aseguramiento de los equipos a través de la póliza general de la Alcaldía Municipal.

En cuanto a los sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales, se brindarán capacitaciones en el uso de herramientas tecnológicas, mantenimiento de equipos, cambios de contraseñas, fireware o cortafuegos, etc. La información de la alcaldía se mantendrá en áreas seguras para el almacenamiento y conservación ubicadas en la Alcaldía y en el archivo central de la Alcaldía Municipal.

19.2 ACCIONES DE SEGURIDAD DE LAS INSTALACIONES Y PUESTOS DE TRABAJO

Se recomienda mantener las puertas cerradas de las oficinas donde se encuentren los equipos de cómputo, los periféricos y todos los medios de almacenamiento, cuando no se encuentren los funcionarios responsables de ellos, y de ser posible, con llave, con el fin de evitar el ingreso de personas ajenas a la Administración Municipal y prevenir posibles hurtos de los citados que puedan comprometer la seguridad de la información almacenada en ellos.

De la misma manera, se recomienda mantener abierta la puerta de acceso principal a las instalaciones únicamente dentro del horario establecido para la atención al público. Al finalizar cada jornada de trabajo y/o al iniciarse el receso correspondiente al almuerzo, debe de estar cerrada esa puerta.

19.3 ACCIONES SOBRE LA UBICACIÓN Y EL ENTORNO DE USO DE LOS EQUIPOS DE CÓMPUTO

Todos los equipos de cómputo, los periféricos y los medios de almacenamiento deben ser usados conforme lo describen los manuales de uso correspondientes y se recomienda que su ubicación sea segura, es decir, lejos de contaminantes, de cualquier elemento peligroso –combustibles, químicos, entre otros, de la humedad y de cualquier superficie que no sea segura incluso para el mismo responsable del equipo.

Se debe tener a mano un extintor de incendios en los puestos de trabajo, debidamente cargado y ubicado en un lugar de fácil acceso. Los usuarios deben comunicar de manera inmediata al responsable de Sistemas cuando detecten posibles riesgos por factores como la humedad, inundaciones, choques eléctricos, robos, sobrecalentamientos, etc.

19.4 ACCIONES SOBRE LA LIMPIEZA Y EL MANTENIMIENTO DE LOS EQUIPOS DE CÓMPUTO.

Todo equipo de cómputo debe limpiarse conforme lo indique el fabricante, y de ser posible, no con agua ni con jabones detergentes, sino con productos especializados para la limpieza de tales elementos.

Se recomienda que los equipos de cómputo y los periféricos sean protegidos con unas fundas especializadas para evitar el ingreso de contaminantes a su conjunto.

Los usuarios no están autorizados para instalar o desinstalar dispositivos, o hacer mantenimiento a los equipos sin previa autorización del responsable de la Dependencia de Sistemas, en caso de que requieran asistencia técnica de primera instancia deben dar aviso al responsable de sistemas o a su superior inmediato para que brinde esa asistencia y agotar la instancia, cuando el daño sea mayor, el responsable de la oficina de Sistemas deberá hacer los trámites correspondientes para que el equipo sea llevado a un centro de servicio autorizado.

20. GESTIÓN DE ACTIVOS

20.1 INVENTARIO DE ACTIVOS

El conocimiento, uso y propiedad de los activos de información en la entidad, permite generar valor agregado efectuando control y protección a sus procesos, contando con el pleno conocimiento de lo que la Alcaldía posee para el desarrollo de su misión y visión y evitando así incumplimiento de responsabilidades, violación a los derechos de autor y responsabilidades derivadas por la pérdida o daño de los mismos.

La alcaldía ha designado un responsable en cada dependencia para clasificar, elaborar y mantener actualizado un inventario de activos de información, con el fin de garantizar la disponibilidad, integridad y confidencialidad de estos. De igual forma, que permita al activo de información ser identificado, teniendo un dueño o propietario que establezca permisos para su acceso.

20.2 USO ACEPTABLE DE LOS ACTIVOS

Los activos de información de la Alcaldía Municipal, tales como hardware, software, aplicaciones, servicios, información (bases de datos, archivos de datos, contratos, acuerdos, planes, entre otros) son para uso exclusivo del cumplimiento de los objetivos misionales y debe dársele un uso ético, racional y responsable.

Para realizar consultas de documentos que reposan en las oficinas de la Alcaldía Municipal, se permitirá en días y horas laborales, con la presencia del funcionario responsable o custodio de la información; Con excepción de los expedientes contractuales que reposan en la Unidad de Contratación, los cuales serán puestos a disposición en medio magnética.

21. PRIVACIDAD DE LA INFORMACIÓN

Es importante para la Alcaldía Municipal de Quibdó la salvaguardia de la privacidad de la información personal del usuario obtenida a través del Sitio web, para lo cual se compromete a adoptar una política de confidencialidad de acuerdo con lo que se establece a continuación:

El Usuario reconoce que el ingreso de información personal, lo realiza de manera voluntaria y ante la solicitud de requerimientos específicos por la Alcaldía para realizar un trámite, presentar una queja o reclamo, o para acceder a los mecanismos interactivos.

La recolección y tratamiento automatizado de los datos personales, como consecuencia de la navegación y/o registro por el Sitio Web tiene como finalidades las detalladas a continuación: la adecuada gestión y administración de los servicios ofrecidos en el sitio web, en los que el usuario decida darse de alta, utilizar o contratar; el estudio cuantitativo y cualitativo de las visitas y de la utilización de los servicios por parte de los usuarios; el envío por medios tradicionales y electrónicos de información relacionados con la Alcaldía y sus programas y sus entidades adscritas y vinculadas; poder tramitar servicios de gobierno en línea.

La Alcaldía Municipal no cederá a terceros los datos personales de los usuarios que se recogen a través de la página web sin su consentimiento expreso. Sin perjuicio de lo anterior, el usuario consiente en que se cedan sus datos personales cuando así sea requerido por las autoridades administrativas competentes o por mandato judicial.

El usuario también comprende que los datos por él consignados harán parte de un archivo y/o base de datos que podrá ser usado por la Alcaldía para efectos de surtir determinado proceso. El usuario podrá modificar o actualizar la información suministrada en cualquier momento.

La Alcaldía Municipal no se responsabiliza por cualquier consecuencia derivada del ingreso indebido de terceros a la base de datos y/o por alguna falla técnica en el funcionamiento y/o conservación de datos en el sistema en cualquiera de los menús de su página web.

La construcción de estas políticas para la Alcaldía Municipal se ayuda con las publicadas en la página www.mintic.gov.co, adecuadas y modificadas para la Alcaldía.

MARCO LEGAL

El Artículo N° 20 de la Constitución Política de Colombia de 1991 establece que “Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.”

El Artículo N° 67 dispuso que “la educación es un derecho de la persona y un servicio público que tiene una función social; con ella se busca el acceso al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura. La educación formará al colombiano en el respeto a los derechos humanos, a la paz y a la democracia; y en la práctica del trabajo y la recreación, para el mejoramiento cultural, científico, tecnológico y para la protección del ambiente.”

La Ley 1341 de 2009 Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones en el artículo 38 sobre Masificación del uso de las TIC y cierre de la brecha digital establece que “El Ministerio de Tecnologías de la Información y las Comunicaciones, revisará, estudiará e implementará estrategias para la masificación de la conectividad, buscando sistemas que permitan llegar a las regiones más apartadas del país y que motiven a todos los ciudadanos a hacer uso de las TIC. Parágrafo. Las autoridades territoriales implementarán los mecanismos a su alcance para gestionar recursos a nivel nacional e internacional, para apoyar la masificación de las TIC, en sus respetivas jurisdicciones.”

El Decreto 2573 de 2014, Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, TÍTULO. II Artículo 5 - Componentes. Los fundamentos de la Estrategia serán desarrollados a través de 4 componentes que facilitarán la masificación de la oferta y la demanda del Gobierno en Línea.

Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Capítulo Primero: de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. Capítulo Segundo: De las atentados informáticos y otras infracciones.

Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013, por la cual se dictan disposiciones generales para la protección de datos personales. Artículo 2. Tratamiento de datos en el ámbito personal o doméstico. De conformidad con lo dispuesto en el literal a) del artículo 2 de la Ley 1581 de 2012, se exceptúan de la aplicación de dicha Ley y del presente Decreto, las bases de datos mantenidas en un ámbito exclusivamente personal o doméstico. El ámbito personal o doméstico comprende aquellas actividades que se inscriben en el marco de la vida privada o familiar de las personas naturales.

En Colombia existe normatividad que reglamenta y propende por la implementación de medidas de seguridad y privacidad de la información, como el 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.

Igualmente en la Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales y que tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Decreto 415 de 2016, Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

Política SGSI Modelo de Seguridad de la Información para la estrategia de Gobierno en Línea, Modelo que emite el Ministerio TIC en temas del Modelo de Gestión de Seguridad de la Información.

GLOSARIO

CONFIDENCIALIDAD: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

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 organización antes de crear nuevas políticas.

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.

HARDWARE: componentes físicos del ordenador, es decir, todo lo que se puede ver y tocar.

LAN: es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

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 organización.

PROCEDIMIENTO: se 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.

RIESGO: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

ROUTER: se trata de un producto de hardware que permite interconectar computadoras que funcionan en el marco de una red a través de varias conexiones (LAN y wifi).

SOFTWARE: estos son los programas informáticos que hacen posible la realización de tareas específicas dentro de un computador.

SWITCHES: son los encargados de la interconexión de equipos dentro de una misma red, o lo que es lo mismo, son los dispositivos que, junto al cableado, constituyen las redes de área local o LAN.

TROYANO: aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

USUARIO: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la alcaldía municipal.

VIRUS: Los virus son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta. Estos, por lo general, infectan otros archivos del sistema con la intensión de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador.

VULNERABILIDAD: debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

REFERENCIAS BIBLIOGRÁFICAS

Capítulo IV referente a la Gestión de Documentos Electrónicos de Archivo del Decreto 2609 de 2012, por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Decreto 2693 de 2012, por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de gestión de la seguridad de la información (SGSI). Bogotá: ICONTEC, 2004, 67 p.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information Technology. Security Techniques. Information Security Management Systems. Requirements. Geneva, ISO. pp 34 (ISO/IEC 27001: 2005)

Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 de 2009 Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones en el artículo 38 sobre Masificación del uso de las TIC y cierre de la brecha digital.

Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013, por la cual se dictan disposiciones generales para la protección de datos personales.

OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN. Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional. 1 ed. Buenos Aires: ONTI, 2005.