MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MUNICIPIO DE DOSQUEBRADAS

ELABORÓ MONICA ORREGO CEBALLOS

Versión: 1

TABLA DE CONTENIDO

INTRODUCCIÓN 4
1. GENERALIDADES 5
1.1 Objetivo 5
1.2 Alcance 5
1.3 Obligaciones 5
1.4 Propósito 5
1.5 Marco Legal: 5
1.6 Advertencia 8
1.7 Definiciones 8
1.8 Acuerdos de Confidencialidad y Derechos de Propiedad Intelectual 14
2. CLASIFICACIÓN DE LA INFORMACIÓN 14
2.1 Responsable de la Clasificación 15
2.2 Nivel de Protección 15
3 POLÍTICAS ESPECÍFICAS DE LA SEGURIDAD DE LA INFORMACIÓN 15
3.1 Políticas para Cuentas de Usuario de los Sistemas 15
3.2 Políticas para Seguridad de la Red Interna y Perimetral 16
3.3 Políticas para el Buen Uso y Cuidado de los Recursos Informáticos 16
3.4 Política para Acceso Físico a Áreas Sensibles 18
3.5 Política para Acceso a los Recursos Informáticos 19
3.6 Política para Gestión de Comunicaciones/Operaciones 22
3.7 Políticas para Correo Electrónico, Internet, Web E Intranet 24
3.8 Políticas para Seguridad de Recursos Humanos 25
3.9 Política para Retiro Equipos Para Trabajo Externo 25
3.10 Política para Mantenimiento y Conservación de Equipos y Redes 26
3.11 Políticas para la Seguridad en la Reutilización o Eliminación de Equipos 26
3.12 Política para Uso de Dispositivos de Almacenamiento Masivo de Información 27

3.13 Política para Adquisición, Desarrollo y Mantenimiento de Sistemas de Información 27

3.14 Políticas para Incidentes de Seguridad de la Información 28

4 CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 28

5 EXCEPCIONES 29

INTRODUCCIÓN

La Alcaldía de Dosquebradas, consciente de los avances tecnológicos y su importancia en el cumplimiento de sus objetivos para poder así prestar un buen servicio a la ciudadanía, reconoce en la información un componente indispensable para la consecución de los objetivos, misión y visión, por lo tanto se le debe dar un tratamiento seguro, bajo la supervisión de los Secretarios, Directores, Jefes de área y la responsabilidad de cada uno de los funcionarios de la entidad; con el fin de mantener la confidencialidad, integridad, y disponibilidad de la misma.

Por esta razón y en cumplimiento de un deber legal se desarrolla la presente política de seguridad informática, para asegurar que la información sea protegida de forma adecuada desde su recolección pasando por el manejo procesamiento y almacenamiento. Esta política establece y describe los parámetros y lineamientos de la seguridad digital. Igualmente al hablar de seguridad digital se incluirán los conceptos sobre seguridad de la información, seguridad informática, ciberseguridad y protección de datos personales.

Para su elaboración se basan en los parámetros definidos por el Ministerio de las Tecnologías y las Comunicaciones, leyes y normas aplicables, y con base en estas políticas se establecerán controles a los diferentes riesgos que puedan afectar la administración de la Alcaldía de Dosquebradas, entendiendo que esta se encuentra conformada por los empleados de carrera, contratistas y colaboradores y es responsabilidad de todos velar por la seguridad digital.

1. GENERALIDADES

1.1 Objetivo

Establecer reglas y lineamientos técnicos para el uso controlado de activos informáticos, que garanticen la seguridad de la información minimizando así el riesgo de pérdida de datos, accesos no autorizados, divulgación no controlada, duplicación e interrupción intencional de la información.

1.2 Alcance

Las Políticas de Seguridad Informática de la Alcaldía del Municipio de Dosquebradas incluye todos los procesos, funcionarios y contratistas de las distintas Secretarías que componen la estructura de la Entidad. Incluye los lineamientos para proteger la información de la Alcaldía y los recursos tecnológicos con la que se procesa y se almacena, así como la recuperación de la información mantenida a nivel de medios (discos, memorias, entre otros) para responder a los requerimientos de los procesos de la entidad.

1.3 Obligaciones

Es un compromiso de todos los funcionarios, contratistas, aprendices y terceros vinculados a la Alcaldía del Municipio de Dosquebradas, conocer las Políticas de Seguridad informática y es su deber cumplirlas y respetarlas para el desarrollo de cualquier actividad o consulta de sus productos.

1.4 Propósito

El propósito que tiene la Alcaldía del Municipio de Dosquebradas al establecer las políticas de Seguridad Informática, es definir las normas y lineamientos a través de este documento para que la gestión de proyectos y recursos informáticos se realice obedeciendo la directriz de seguridad y evitar que se creen vulnerabilidades que impacten la actividad de la Entidad.

1.5 Marco Legal:

El presente documento se encuentra apoyado en la siguiente normatividad vigente para el proceso de políticas de la información:

Constitución Política de Colombia:

Artículos 2°, 29°, 74°, 78°, 83°, 315°

Ley 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 734 de 2002: "Código Único Disciplinario**"**

Ley 1273 de 2009: "Por medio del 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".

Artículo 269a: Acceso abusivo a un sistema informático.
Articulo 269b: Obstaculización ilegítima de sistema informático o red de telecomunicación.
Articulo 269c: Interceptación de datos informáticos.
Articulo 269d: Daño Informático.
Articulo 269e: Uso de software malicioso.
Articulo 269f: Violación de datos personales.
Articulo 269g: suplantación de sitios web para capturar datos personales.
Articulo 269h: Circunstancias de agravación punitiva.
Articulo 269i: Hurto por medios informáticos y semejantes
Articulo 269j: Transferencia no consentida de activos.

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 del Espectro y se dictan otras disposiciones**".**

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".

Ley 2609 de 2012: "reglamenta el titulo V de la Ley General de Archivo año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos".

Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Trasparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones**".**

Decreto 1151 de 2008: “Por medio del cual se establecen los lineamientos generales de la política Gobierno en Línea de la República de Colombia, se reglamente parcialmente la Ley 962 de 2005 y se dictan otras disposiciones.”

Decreto 2693 de 2012 "Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones".

Decreto 2573 de 2014: “Por medio del cual se establecen los lineamientos generales de la estrategia de Gobierno en Línea, se reglamenta parcialmente la ley 1341 del 2009 y se dictan otras disposiciones”.

Decreto 1078 de 2015 “Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1008 de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el cap 1 del título 9 a la parte 2 del libro 2 del Decreto 1078/2015 del Sector de Sector de Tecnologías de la Información y las Comunicaciones.

Documento CONPES 3701 Lineamientos de política para ciberseguridad y ciberdefensa

Documento CONPES 3854 Política Nacional de Seguridad Digital.

Estándares:

NTCGP 1000:2009: Norma técnica de calidad en la gestión pública.

Normas ISO/IEC 27000:

NORMA ISO / IEC	TITULO
ISO 27000	Gestión de la Seguridad de la información: Fundamentos y vocabulario.
ISO 27001	Especificaciones para SGSI

ISO 27002	Código de buenas prácticas
ISO 27003	Guía de implantación de un SGSI
ISO 27004	Sistemas de métrica e Indicadores
ISO 27005	Guía de análisis y gestión de riesgos
ISO 27006	Especificaciones para Organismos Certificadores SGSI

1.6 Advertencia

Cualquier cliente de los recursos de TIC de la Alcaldía del Municipio de Dosquebradas que se encuentre realizando actividades que vayan en contra de las Políticas de Seguridad Informática, da lugar a que la Entidad realice las investigaciones disciplinarias pertinentes y reportar a los entes de control del estado cuando haya lugar.

La utilización indebida de perfiles de usuarios para obtener beneficio propio o en favor de terceros será sancionado de acuerdo con los procedimientos administrativos definidos.

1.7 Definiciones

ACTIVO DE LA INFORMACIÓN: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de la entidad y en consecuencia, debe ser protegido.

APLICACIONES CRÍTICAS: Son las aplicaciones o sistemas de información que reciben este término porque previamente se encuentran clasificados como vital o necesarias para el buen funcionamiento de los procesos y procedimientos misionales.

AUTENTICACIÓN: es el procedimiento de comprobación de la Entidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

BRECHA: Término que se utiliza para denominar la diferencia que se observa entre el mecanismo de seguridad que existe y la situación ideal para evitar que germinen vulnerabilidades que impacten el negocio de la Entidad.

BUENAS PRÁCTICAS: Son lineamientos que contiene los principios básicos y generales para el desarrollo de los productos o servicios de la organización para la satisfacción al cliente.

CIBERAMENAZA O AMENAZA CIBERNÉTICA: aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.

CIBERATAQUE O ATAQUE CIBERNÉTICO: acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.

CIBERESPACIO: entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.

CIBERIESGO O RIESGO CIBERNÉTICO: posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.

CIBERSEGURIDAD: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la Entidad.

CLASIFICACIÓN DE LAS APLICACIONES: Las aplicaciones se clasifican conforme los procesos de la entidad y son: Misional, Estratégico y de Apoyo

CLASIFICACIÓN DE LA INFORMACIÓN: Proceso formal que se utiliza para ubicar el nivel a la información de la Entidad con el fin de protegerla; previa estructura de valoración en atención al riesgo que se presume existe si hay una divulgación no autorizada. Generalmente la información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.

CLIENTES: Persona natural o usuario que recibe un producto Institucional. El cliente puede ser interno o externo a la organización.

CORRIENTE ELÉCTRICA REGULADA: Se utiliza para regular o mantener el voltaje de la red eléctrica para que no afecte el funcionamiento de los recursos TIC de la Entidad.

CONTROL: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

DATO: Es una letra, número o símbolo que tiende a convertirse en información.

DOCUMENTO: Es el medio físico que contiene la información que se quiere transmitir.

EVENTO DE SEGURIDAD: ocurrencia de una situación que podría afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.

FUNCIONARIO GENERADOR DE LA INFORMACIÓN: Es cualquier persona que es propietaria de la información y tiene la responsabilidad de custodiarla.

INCIDENTE DE SEGURIDAD: ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la Entidad que son esenciales para el negocio.

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

INFORMACIÓN DIGITAL: Cuando la información está almacenada en un medio magnético porque cuando se imprime se convierte en documento físico.

INFORMACIÓN SENSIBLE: Es la tipificación que recibe la información que no se considerada de acceso público como por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos. En el entorno de seguridad informática se considera usar este término para designar datos privados relacionados con Internet o la informática, sobre todo contraseñas, tanto de correo electrónico, conexión a Internet, IP privada, sesiones del PC, etc.

INVENTARIO DE ACTIVOS DE INFORMACIÓN: es una lista ordenada y documentada de los activos de información pertenecientes a la entidad, estos comprenden software y hardware.

POLÍTICA TIC: Documento que contiene los lineamientos que define la organización para reglamentar el desarrollo de los proyectos y recursos TIC de la Entidad; como las acciones que deben permanecer en el tiempo para alcanzar los objetivos de su negocio.

POLITICA DE SEGURIDAD: Es el documento de normas y lineamientos de seguridad de la información que define la Entidad para evitar que surja vulnerabilidades que puede afectar el negocio de la Entidad.

PROVEEDORES: Negocio o empresa que ofrece servicios a otras empresas o particulares. Ejemplos de estos servicios incluyen: acceso a internet, operador de telefonía móvil, alojamiento de aplicaciones web etc.

ENCARGADO DEL PROCESAMIENTO DE LA INFORMACION: Se utiliza para denominar a la persona autorizada para organizar, clasificar y valorar la información de su dependencia o área conforme al cargo de la estructura organizacional de la Entidad.

REPOSITORIO DE DOCUMENTOS: Sitio centralizado donde se almacena y mantiene información digital actualizada para consulta del personal autorizado.

REQUERIMIENTO: Necesidad de un servicio TIC que el usuario solicita a través del mecanismo definido por la organización en los procedimientos normalizados.

SECRETARÍAS: Son los grupos que conforman la estructura organizacional de la Entidad.

SERVICIO: Incluye los servicios profesionales para la instalación, mantenimiento, desarrollo, integración de software y adquisiciones, enajenaciones, arrendamientos y contratación de Hardware y soporte tanto de software como de hardware; así como de la Plataforma Tecnológica.

SERVICIOS TIC: El concepto de Servicio TIC consiste en dar soporte, de forma integrada y personalizada, a todas estas herramientas que necesita hoy en día el profesional de empresa para realizar su trabajo. Los elementos del Servicio TIC son:

- Los dispositivos: PC, portátiles, agendas electrónicas, impresoras, teléfonos, sistemas de videoconferencia, etc

- La Red de Área Local corporativa (LAN). Así como las comunicaciones de voz incluyendo el teléfono y ahora llega el momento de proporcionar y gestionar los PC y la electrónica de red necesarios para las comunicaciones de datos.

- Las comunicaciones de voz y datos WAN (Red de Área Remota), que incluyen tanto las redes privadas corporativas como el acceso a redes públicas como Internet. La integración de las comunicaciones WAN y estas cada vez se requieren con las comunicaciones LAN.

- Los servicios y aplicaciones desde la red. Existe una clara tendencia hacia la "externalización" de determinados servicios de acuerdo a la madurez y sus problemas conocidos y controlados. Un ejemplo es el correo electrónico. Muchas empresas prefieren "externalizar" este servicio para no tener que dedicar recursos a mantener y gestionar la infraestructura de correo durante las 24 horas los 7 días de la semana.

SGSI: Sistema de Gestión de Seguridad de la Información. Concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización, que debe tener la política, estructura organizativa, procedimientos, procesos y recursos necesarios para implantar la gestión de la seguridad de la información.

SISTEMA DE INFORMACIÓN: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

TIC: Conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información, en la actualidad no solo una computadora hace referencia al procesamiento de la información. Internet forma parte de ese procesamiento que, quizás, se realice de manera distribuida y remota.

El procesamiento remoto, además de incorporar el concepto de telecomunicación, hoy día hace referencia a un dispositivo como un

teléfono móvil o una computadora ultra-portátil, con capacidad de operar en red mediante Comunicación inalámbrica.

USUARIO: Persona que utiliza los recursos TIC y que interactúan de forma activa en un proceso, secuencia, código etc.

Los jefes de despacho de cada secretaría en la Alcaldía municipal son los responsables de identificar y valorar su información. Todos los servidores públicos deben seguir los lineamientos enmarcados en este documento

La seguridad de la información debe estar enmarcada con los siguientes principios:

AUDITABILIDAD: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

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

CONFIABILIDAD DE LA INFORMACIÓN: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

CONFIDENCIALIDAD: Se garantiza que la información sea accesible sólo a aquellas personas que estén autorizadas para tener acceso a ella.

DISPONIBILIDAD: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

INTEGRIDAD: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

LEGALIDAD: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

NO REPUDIO: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

PROTECCIÓN A LA DUPLICACIÓN: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.

Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

1.8 Acuerdos de Confidencialidad y Derechos de Propiedad Intelectual

Mientras persista una relación laboral con la Alcaldía, todos sus funcionarios cederán a ésta los derechos de propiedad intelectual de los desarrollos que originen como parte de sus responsabilidades laborales con la Alcaldía.

Siempre que se requiera compartir información "**Pública Clasificada**" y/o "**Pública Reservada**" con un tercero, deberá acogerse a los términos de la Ley.

2. CLASIFICACIÓN DE LA INFORMACIÓN

La información propiedad de la Alcaldía de Dosquebradas se considerará por defecto como "**Interna**", correspondiente a toda la información no "**Pública**", o que no haya sido declarada como "**Publica**", "**Publica Clasificada**" o "**Pública Reservada**". (Ley 1712 de 2014 de Trasparencia, Articulo 6) Sólo se podrá tener acceso a información clasificada como "**Publica Clasificada**" o "**Publica Reservada**" bajo previa aprobación del "sujeto obligado" de la información. (Art. 5 Ley 1712/2014)

De acuerdo a la Ley en Mención, la información se clasifica en:

- **Pública**: Toda obligación que un sujeto obligado genere, obtenga, adquiera o controle en su calidad de tal.

- **Pública Clasificada**: Es aquella información, que estando en poder o custodia de un sujeto obligado, pertenece al ámbito propio, particular y privado o semi privado, de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la citada Ley.

- **Pública Reservada**: Es aquella información, que estando en poder o custodia de un sujeto obligado o en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo el cumplimiento de la totalidad de los requisitos consagrados en el Artículo 19 de la citada Ley.

2.1 Responsable de la Clasificación

La responsabilidad de la clasificación de la información, recae sobre los Secretarios de Despacho, Directores Operativos, Asesores y Jefes de Área de cada dependencia. Se debe tomar como guía para el proceso de clasificación, lo establecido en la Ley 1712 del 2014 Articulo 6**.**

2.2 Nivel de Protección

El nivel de protección requerido para cada nivel de clasificación, se deberá evaluar analizando los requerimientos de Confidencialidad (la información de mayor valor para la entidad solo puede ser conocida por personas autorizadas); e Integridad (la información no debe poder ser alterada o destruida de manera no autorizada para afectar la entidad).

3 POLÍTICAS ESPECÍFICAS DE LA SEGURIDAD DE LA INFORMACIÓN

3.1 Políticas para Cuentas de Usuario de los Sistemas

- El acceso a los sistemas de información será controlado por medio de nombres de usuario y contraseñas personales e intransferibles. Está prohibido el préstamo de cuentas (revelación de contraseñas) de los sistemas (aplicaciones, equipos, correo electrónico etc.).

- Sólo se crearán cuentas de usuario genéricas en los sistemas de información, si las mismas contemplan exclusivamente opciones de consulta, bajo la condición de que no se esté accediendo a información clasificada como "**Información Pública Reservada**" definida en la Ley 1712 de 2014(Ley de Trasparencia, Articulo 6 Literal c).

- Los usuarios deben establecer contraseñas que no sean fácilmente identificables, que contengan letras, números y símbolos.

- Las contraseñas de acceso a los sistemas de información no deben ser escritas en medios físicos o digitales no protegidos (deben ser memorizadas o almacenadas digitalmente: bajo técnicas de cifrado de datos, o usando archivos protegidos por contraseñas fuertes), ni deben ser dejadas en lugares visibles.

- Cuando se produzcan cambios de funciones que impliquen la reasignación de privilegios sobre los sistemas, se deben tramitar oportunamente los cambios de permisos bajo responsabilidad de los jefes de los funcionarios.

- Toda desvinculación de funcionarios de la entidad, deberá ser comunicada por el jefe del funcionario a La Dirección de talento humano con el fin de cancelar los accesos a los sistemas de información y recuperar los activos informáticos asignados.

- Las contraseñas de los usuarios administradores de las plataformas tecnológicas y sistemas de la compañía deberán ser salvaguardados bajo custodia del Director de la Dirección de Tecnologías de la Información y las Comunicaciones o quien este delegue, en un archivo protegido a través de técnicas de cifrado de datos u otro mecanismo seguro.

3.2 Políticas para Seguridad de la Red Interna y Perimetral

- La creación de cuentas de usuario para acceso remoto a la red interna de la Alcaldía a través de VPN, sólo será autorizada por el Director de la Dirección de Tecnologías de la Información y las Comunicaciones.

- La red interna deberá estar protegida de amenazas externas, a través de sistemas que permitan implementar reglas de control de tráfico desde y hacia la red de la Alcaldía.

- No está permitida la conexión a la red interna de equipos diferentes a los asignados por la Alcaldía. En caso de existir la expresa necesidad de conectar un equipo de un tercero, solo podrá realizarse bajo previa autorización del Director de la Dirección de Tecnologías de la Información y las Comunicaciones.

- Todas las redes inalámbricas existentes en la entidad deberán cumplir con los Estándares de Seguridad definidos por la Dirección de Tecnologías de la Información y las Comunicaciones.

3.3 Políticas para el Buen Uso y Cuidado de los Recursos Informáticos

- La Alcaldía del Municipio de Dosquebradas debe definir los mecanismos para proteger la información, su uso, procesamiento, almacenamiento, difusión; y, es su deber, mantener actualizada la presente política de seguridad de la información.

- La Alcaldía del Municipio de Dosquebradas, debe dar los lineamientos para clasificar, valorar y dar tratamiento a los recursos tecnológicos involucrados

- Los equipos informáticos fijos y portátiles asignados por la Alcaldía a sus funcionarios, son herramientas de trabajo y deben ser utilizados para fines laborales. El usuario a quien le hayan sido asignados será responsable de su buen cuidado y correcto uso.

- Todos los sistemas de información y recursos tecnológicos utilizados para el procesamiento deben contar con mecanismo de seguridad apropiados.

- Toda la información almacenada en los equipos de cómputo son, en principio, propiedad de la Alcaldía, y debe ser clasificada de acuerdo con las normas definidas en esta Política. La información "**Personal**" almacenada en estos equipos deberá estar claramente identificada y separada de la información laboral.

- La información pública de la Alcaldía no debe ser copiada en equipos personales.

- No está permitida la instalación de ningún software adicional al aprobado por el Director de la Dirección de Tecnologías de la Información y las Comunicaciones. Igualmente está prohibido descargar software de uso malicioso o documentos que brinden información que atente contra la seguridad de la información de la Alcaldía.

- Ningún usuario de los recursos informáticos debe visitar sitios restringidos por la entidad de manera explícita o implícita, o sitios que afecten la productividad en la Institución; como el acceso desde la Entidad a sitios relacionados con la pornografía, juegos, redes sociales, etc.

- Todos los usuarios de los recursos informáticos deben proteger, respaldar y evitar accesos de la información a personas no autorizadas; es decir, son responsables de cuidar todos los activos digitales de información propiedad de la entidad.

- Todo usuario de equipos informáticos debe bloquear la sesión de trabajo de su computador al alejarse aunque sea por poco tiempo, minimizando el tiempo que la estación quede sin protección en su ausencia.

- Todo usuario de Equipos informáticos es responsable de la protección de la información a su cargo y no debe compartir, publicar o dejar a la vista, datos como Usuario y contraseñas

- El usuario es responsable de realizar las copias de seguridad requeridas para proteger la información almacenada en los equipos asignados.

- Ningún usuario de los recursos informáticos debe generar, compilar, copiar, almacenar, replicar o ejecutar código de computador malicioso con la intención de causar daño, afectar e interferir con los servicios de cualquier recurso o con el pretexto de encontrar vulnerabilidades al sistema, so pena de las sanciones pertinentes.

- Ningún funcionario está autorizado para compartir o brindar información de su equipo sin establecer restricciones a personas ya sean internas o externas a la Entidad.

- Toda información que provenga de un archivo externo de la Entidad o que deba ser restaurado tiene que ser analizado con el antivirus institucional vigente.

3.4 Política para Acceso Físico a Áreas Sensibles

- La Alcaldía del Municipio de Dosquebradas debe garantizar la seguridad física en todas las secretarías de la Entidad para prevenir e impedir accesos no autorizados, daños e interferencia a las instalaciones así como a la información que recibe y genera la entidad.

- La Alcaldía del Municipio de Dosquebradas a través de las diferentes dependencias debe identificar y garantizar el control de los aspectos ambientales que pueden llegar a interferir el correcto funcionamiento de los recursos tecnológicos inherentes en el procesamiento y almacenamiento de la información institucional.

- Todas las secretarías de la Alcaldía Municipal deben definir los niveles de seguridad física y de acceso a las instalaciones y puestos de trabajo de las oficinas que están bajo su responsabilidad y como encargados del procesamiento de la información son los encargados de aprobar o negar la autorización formal del acceso a las oficinas de su competencia cuando sea requerido.

- Las áreas definidas como sensibles por su nivel de procesamiento de información (centros de cómputo), deberán contar con controles físicos que impidan el acceso de personal no autorizado. Los terceros siempre deberán permanecer acompañados por un funcionario de la Dirección de Tecnologías de la Información y las Comunicaciones.

- Todos los recursos físicos inherentes a los sistemas de información de La Alcaldía del Municipio de Dosquebradas como las instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc. deben estar protegidos para evitar que personal ajeno tengo acceso a ellos y puede generar vulnerabilidades o amenazas a los sistemas y la información.

- Los recursos informáticos utilizados para el procesamiento de la información deben estar ubicados en sitios estratégicos con mecanismos de seguridad que permita controlar el acceso solo a las personas autorizadas e incluir en la protección de los mismos los traslados por motivos de mantenimiento u otros escenarios.

- Todos los funcionarios de la Entidad son responsables del uso adecuado de las pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario que realiza.

3.5 Política para Acceso a los Recursos Informáticos

La Alcaldía de Dosquebradas, en busca de garantizar un adecuado control de acceso a sus activos de información, ha definido las políticas para garantizar un adecuado control de acceso a los sistemas, para ello se implementan mecanismos de control para acceder a la red, sistemas operativos, bases de datos, sistemas de información y en general a todo elemento que de alguna forma acceda o permita el acceso a información de carácter público reservado o publico clasificado, cuyo origen sea La Alcaldía de Dosquebradas. De igual manera, implementa procedimientos para la asignación de privilegios de acceso a los sistemas.

El acceso a la información contempla el establecimiento de permisos específicos para leer, escribir, modificar, borrar o ejecutar utilidades que procesen información institucional.

- Los funcionarios que manejen sistemas de información, deben solicitar a la Dirección de Tecnología, las credenciales de acceso de las plataformas y velar por la seguridad de estas.

- La Dirección de Tecnología, debe documentar y revisar los procedimientos para administrar y controlar el acceso a los sistemas y recursos tecnológicos de la Entidad de acuerdo a las necesidades de seguridad y de sus actividades

- Cada secretaría es responsable de mantener la integridad y confidencialidad

- Todo usuario de los recursos informáticos debe notificar a la Director de la Dirección de Tecnologías de la Información y las Comunicaciones o a quien corresponda, el tipo de información que requiere medidas específicas de protección para evitar el acceso al personal no autorizado.

- Todos los funcionarios que utilicen medios de almacenamiento de información como CDs, Dvds, Memorias USB, Portátiles, Discos externos, primero deberá acreditar la necesidad de uso a la Dirección de Tecnología para el uso de estos dispositivos y deberán cumplir las siguientes recomendaciones:

  - Analizar con el antivirus todos los dispositivos extraíbles que contengan información externa de la entidad.
  - Extraer de forma segura los dispositivos extraíbles.
  - Verificar el estado físico de los medios de almacenamiento extraíble, para evitar daños al equipo informático

- La Dirección de Tecnología, debe documentar de manera formal la administración de Contraseñas de Usuario de acceso a los sistemas de información y de aquellas con las cuales se realizan actividades como instalación de plataformas, habilitación de servicios, actualización de software, configuración de componentes informáticos, entre otros; y, que deben encontrarse protegidas por contraseñas con un mayor grado de complejidad de seguridad.

- Los usuarios deben seguir y aplicar las buenas prácticas de seguridad para la selección y uso de contraseñas que la Dirección de Tecnologías de la Información y las Comunicaciones, implante y documente.

- La Dirección de Tecnología, debe reglamentar el acceso y el personal autorizado para el ingreso a las estaciones de trabajo o servidores.

- La Dirección de Tecnología, debe documentar los controles de seguridad que contribuya a disminuir el riesgo de acceso no autorizado a los servicios de red.

- La Dirección de Tecnología, debe documentar y controlar la conexión remota y el acceso a los sistemas de información de la Entidad con el fin de minimizar el riesgo de accesos no autorizados.

- La Dirección de Tecnología, debe administrar, controlar y documentar los perímetros de seguridad que implemente mediante la instalación y configuración de “firewall” o redes privadas virtuales, para filtrar el tráfico entre los dominios y bloquear el acceso no autorizado.

- La Dirección de Tecnología, debe implementar controles relacionados con el ruteo de redes, las conexiones informáticas y los flujos de información. Estos controles deben verificar positivamente las direcciones de origen y destino así como los dispositivos de red tales como Hubs, Switches, Bridges, Módems o Routers que tenga la plataforma tecnológica en la Entidad.

- Todos los funcionarios deben aplicar la desconexión por tiempo sin uso temporal de los computadores personales activos en las oficinas o que se active el protector de pantalla con contraseñas y evite el acceso no autorizado, sin cerrar las sesiones de aplicación o de red si debe abandonar su puesto de trabajo momentáneamente. De igual forma, se debe definir limitaciones en el tiempo de conexión que proporcionen un nivel de seguridad adicional a las aplicaciones de alto riesgo.

- La Dirección de Tecnología, debe evaluar los sistemas y determinar los que son sensibles y requieren de un ambiente informático dedicado o aislado o que sólo debe compartir recursos con los sistemas de aplicación confiables o no tener limitaciones.

- La Dirección de Tecnología, debe documentar reglas para el correcto manejo de dispositivos de computación móvil y trabajo remoto que incluyan la protección física necesaria, el acceso seguro y la utilización de los dispositivos en lugares públicos, el acceso a los sistemas de información y servicios a través de estos y la protección contra software malicioso.

- Todos los funcionarios debe solicitar a la Dirección de Tecnologías de la Información y las Comunicaciones o a quien corresponda, la autorización para el trabajo remoto con los sistemas de información de la alcaldía.

- Evitar hacer uso de redes inalámbricas de uso público inseguras para transmitir información institucional, así como conectar los dispositivos (portátiles) a equipos de uso compartido público (café internet, hoteles, computadores personales no institucionales).

- La Dirección de Tecnología, con la solicitud de cuentas de usuario debidamente aprobada por cada Secretario de Despacho o Director Operativo, al cual pertenece el solicitante debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados.

3.6 Política para Gestión de Comunicaciones/Operaciones

- La Dirección de Tecnología debe garantizar el correcto funcionamiento y seguridad de las operaciones que se realizan en el Data Center de la Entidad, con relación al procesamiento de la información y comunicaciones.

- La Dirección de Tecnología es la encargada de definir las responsabilidades funcionales y operativas, con relación al Data Center y de que se documente los procedimientos para su gestión y operación.

- La Dirección de Tecnología y los funcionarios encargados de procesar información de cada una de las secretarías, deben definir y documentar los requerimientos para resguardar la información por la cual es responsable.

- La Dirección de Tecnología, debe aprobar el procedimiento relacionado con los servicios para transportar la información cuando sea demandado, de acuerdo a su nivel de criticidad.

- La Dirección de Tecnología debe definir los procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

- La Dirección de Tecnología, debe verificar que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan.

- La Dirección de Tecnología, debe analizar el posible impacto operativo de los cambios previstos y verificar su correcta implementación.

- Los responsables de la gestión operativa y de comunicaciones del Data Center, deben evaluar los riesgos y determinar los controles que se deben implementar y realizar monitoreo de las actividades.

- La Dirección de Tecnología, debe efectuar el monitoreo al crecimiento del volumen de la información de los sistemas que se encuentran en operación en el Data Center y evaluar la capacidad de almacenamiento y procesamiento de los recursos utilizados, con el fin de proyectar el alcance de estos para evitar saturación en los mismos.

- La Dirección de Tecnología, es la encargada de evaluar los posibles cuellos de botella, que puedan generar amenaza a la seguridad o a la continuidad del procesamiento; también debe planificar la acción correctiva que corresponda.

- La Dirección de Tecnología debe definir los controles para la protección contra el software malicioso.

- La Dirección de Tecnología debe definir y documentar el protocolo de resguardo de la información.

- La Dirección de Tecnología, debe llevar el control de los registros tales como los intentos de acceso a los sistemas, tiempo de inicio y cierre del mismo, errores y medidas correctivas tomadas, entre otras actividades.

- La Dirección de Tecnología es la encargada de documentar e implementar los controles de seguridad de los datos y los servicios conectados en las redes de la Entidad.

- La Dirección de Tecnología, es la encargada de administrar y documentar los procedimientos con medios informáticos portátiles, discos, memorias extraíbles entre otros.

- La Dirección de Tecnología es la encargada de definir los procedimientos para la clasificación, manejo y almacenamiento de la Información, restringiendo el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el funcionario encargado del procesamiento de la Información relativa al sistema.

- La Dirección de Tecnología, es la encargada de definir, documentar e implementar los controles relacionados con el uso adecuado del Correo Electrónico para reducir los riesgos de incidentes de seguridad.

3.7 Políticas para Correo Electrónico, Internet, Web E Intranet

- La Dirección de Tecnología, es la encargada de definir y documentar las normas y procedimientos relacionados con el uso adecuado del Correo Electrónico que debe incluir protección de archivos adjuntos de correo electrónico, uso de técnicas para proteger la confidencialidad e integridad, de los mensajes electrónicos, retención de mensajes que se deben almacenar y como deben ser usados en caso de ser requeridos legalmente.

- La Dirección de Tecnología, es la encargada de definir los aspectos operativos para garantizar el correcto funcionamiento del servicio como el tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, definición de los alcances del uso del correo electrónico por parte del personal de la Entidad entre otros.

- Los mensajes de correo electrónico transmitidos a través de las cuentas de correo suministradas por la Alcaldía no se considerarán correspondencia privada, ya que éstas tienen como fin primordial la transmisión de Información relacionadas con las actividades ordinarias de la Alcaldía.

- Los servicios de correo electrónico e Internet e intranet, son herramientas de trabajo brindados por la Alcaldía y deben ser usados para fines laborales.

- Dentro de los horarios de oficina, el Internet deberá ser empleado exclusivamente para fines laborales.

- La página WEB será administrada exclusivamente por la Dirección de Tecnologías de la Información y las Comunicaciones y la publicación de información y contenidos, serán responsabilidad del sujeto obligado quien genera la información.

- La Intranet es la implementación de la tecnología de Internet de tal manera que solo puedan tener acceso los funcionarios de la Alcaldía, la administración de la misma estará a cargo de la Dirección de Tecnologías de la Información y las Comunicaciones y la información y sus contenidos serán responsabilidad del sujeto obligado.

- La Dirección de Tecnologías de la Información y las Comunicaciones será la encargada de bloquear el acceso a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso corporativo mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad.

3.8 Políticas para Seguridad de Recursos Humanos

- La Dirección de Tecnologías de la Información y las Comunicaciones, debe documentar los lineamientos de seguridad que contribuya a reducir los posibles riesgos que el ser humano pueda cometer voluntaria o involuntariamente; que incluye el uso adecuado de instalaciones y recursos tecnológicos para la seguridad de la información.

- La Alcaldía del Municipio de Dosquebradas a través de la Secretaría de Asuntos Administrativos debe informar al personal nuevo que se vincule o contrate en la Entidad la existencia de las Políticas de seguridad de la información e incluir en los contratos de estos últimos, el compromiso de confidencialidad de la información y la responsabilidad en materia de seguridad.

- La Alcaldía del Municipio de Dosquebradas debe capacitar permanentemente a los funcionarios en materia de seguridad de la información y difundir las posibles amenazas y riesgos que afectan los recursos informáticos de la Entidad.

- La Dirección de Tecnologías de la Información y las Comunicaciones deberá generar el Plan de Sensibilización, Capacitación y Comunicación a disposición de la comunidad en general, con el fin de facilitar el acceso a la información respectiva.

- La Dirección de Tecnología, debe realizar permanentemente campañas de seguridad de la información establecidas en el plan de sensibilización, capacitación y comunicación. Estas actividades del plan van dirigidas a todos los usuarios o clientes de los recursos informáticos para evitar que realicen tareas inseguras que conlleven a pérdida y destrucción de información y/o activos informáticos en la alcaldía de Dosquebradas, generando un cambio cultural en cuanto a los recursos o activos informáticos

3.9 Política para Retiro Equipos Para Trabajo Externo

- Al retirar un equipo informático de las instalaciones de la entidad, el funcionario a quien éste le haya sido asignado será responsable de extremar su cuidado. En caso de daño, pérdida o robo, se establecerá su responsabilidad a través de los procedimientos definidos por la ley para tal fin.

- La información Publica Clasificada o Publica Reservada de la entidad no puede ser copiada en medios externos con excepción de aquellos autorizadas por la Ley, en dispositivos asignados por la Dirección de TI para el respaldo de la misma, los cuales sólo deberán ser empleados para este fin. En caso de ser estrictamente necesaria la copia de esta información en medios adicionales y previa autorización del Sujeto Obligado de la información, ésta deberá ser grabada de forma segura: bajo técnicas de cifrado de datos, o como mínimo comprimiéndola con herramientas suministradas por la entidad y estableciendo una contraseña fuerte.

3.10 Política para Mantenimiento y Conservación de Equipos y Redes

- Cuando un funcionario se retire de su puesto de trabajo, deberá asegurar que la información clasificada como "**Publica Clasificada**" o **"Publica Reservada"** no quede expuesta a terceros no autorizados.

- Todos los funcionarios deberán mantener sus equipos de cómputo limpios y aseados. Cuando se requiera de mantenimiento especializado se debe solicitar a la Dirección de Tecnologías de la Información y las Comunicaciones.

- Ningún funcionario debe consumir alimentos ni ingerir líquidos en el sitio donde se encuentre el equipo de cómputo.

- Los equipos de Cómputo deben estar conectados a la Corriente Regulada, para evitar daños severos, por lo tanto las redes de voz, datos y eléctricas deben permanecer en buen estado y deben ser manipuladas únicamente por el personal capacitado para tal fin.

3.11 Políticas para la Seguridad en la Reutilización o Eliminación de Equipos

- Antes de reasignar un equipo de cómputo de un funcionario que almacene en éste información clasificada como "**Publica Clasificada**" o **"Publica Reservada"** (cuando no se trata del mismo cargo y por lo tanto la información

que se maneja es diferente), se debe garantizar un borrado seguro de tal forma que los datos no puedan ser recuperados.

- Todo dispositivo de almacenamiento de información que sea dado de baja debe ser destruido.

- Antes de realizar la venta y/o donación de equipos de cómputo se deben extraer sus medios de almacenamiento. (Norma ISO 27001:2013)

3.12 Política para Uso de Dispositivos de Almacenamiento Masivo de Información

- El uso de dispositivos que permitan el almacenamiento masivo de información en medios externos, como es el caso de equipos de conexión USB y unidades de escritura de CD/DVD, estará restringido debido a que constituye una amenaza que incrementa el riesgo de pérdida de integridad de la información de la entidad (Infecciones de Software Malicioso) y pérdida de confidencialidad de la misma (fuga masiva de información "**Publica Clasificada**" o **"Publica Reservada"**), además del riesgo de fuga de la información.

- Sólo aquellos funcionarios con claras necesidades tendrán habilitados estos dispositivos con la previa autorización. Su uso será exclusivo para almacenamiento o copias de seguridad y este quedará bajo su estricta responsabilidad, en caso de pérdida del dispositivo y fuga o pérdida de información será el directo responsable.

3.13 Política para Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

- La Alcaldía de Dosquebradas por intermedio de la Dirección de Tecnología debe asegurar que se haga el diseño e implementación de los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.

- La información que se encuentra en los sistemas de producción no puede ser disminuida en los niveles de protección ni ser utilizada en ambientes de desarrollo y pruebas, tanto para mantenimiento como el desarrollo de soluciones.

- La información tratada por las aplicaciones aceptadas por la Alcaldía, debe preservar su confiabilidad desde su ingreso, transformación y entrega a las aplicaciones de la Entidad.

- Se debe reglamentar la adquisición de Software e incluir los controles necesarios para verificar licencias y los requerimientos de seguridad del software establecidos.

3.14 Políticas para Incidentes de Seguridad de la Información

- El Dirección de Tecnologías de la Información y las Comunicaciones o quien este delegue, verificará el cumplimiento de las Políticas de Seguridad de la Información apoyado en las herramientas informáticas implementadas en la Alcaldía.

- Los usuarios de los sistemas de información no deben, bajo circunstancia alguna, intentar probar una supuesta debilidad de seguridad de la plataforma informática de la compañía, por cuanto esta acción será interpretada como una falta grave que será analizada de acuerdo con lo establecido en el código de ética.

- Todo el personal de la Alcaldía de Dosquebradas debe mantener informada a la Dirección de Tecnologías de la Información y las Comunicaciones, acerca de la ocurrencia de incidentes de seguridad.

- La Dirección de Tecnología, debe implementar herramientas y mecanismos necesarios para fomentar una buena comunicación entre las dependencias para conocer las posibles debilidades en materia de seguridad, así como de los incidentes ocurridos, con el fin de minimizar sus efectos y prevenir su reincidencia.

- La Dirección de Tecnologías de la Información y las Comunicaciones debe registrar la información de incidentes de seguridad, evaluar e identificar aquellos que son recurrentes o de alto impacto; así como establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

4 CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

1. La divulgación de las Políticas de Seguridad debe ser transmitido e implementado a través de las diferentes secretarías que conforman la Alcaldía de Dosquebradas.

2. Todos los funcionarios de la Alcaldía de Dosquebradas deben estar autorizados por la Secretaría de Asuntos Administrativos y La Dirección de Tecnologías de la Información y las Comunicaciones, para el uso de los recursos informáticos, se debe vigilar el uso adecuado de la información y de toda la plataforma tecnológica.

3. La oficina asesora de las TIC, debe brindar capacitación a toda a la Entidad sobre los riesgos y amenazas que puede tener la información el cual se considera un activo valioso para la entidad y la conveniencia de aplicar las políticas de seguridad Informática para evitar vulnerabilidades que impacten a la entidad.

4. La oficina asesora de las TIC, es la encargada de socializar en todas las dependencias los lineamientos aprobados por el Comité Interinstitucional de Gestión y Desarrollo sobre Gobierno Digital, Seguridad y Privacidad de la Información y Anti trámites sobre los procedimientos de gestión de riesgos, implementación de políticas, mecanismos de control para mejoras en materia de seguridad de la información en la entidad.

5. Todas las dependencias deben adoptar y cumplir las normas y lineamientos que emita el Comité Interinstitucional de Gestión y Desarrollo sobre Gobierno Digital, Seguridad y Privacidad de la Información y Anti trámites para la administración de las copias de seguridad.

5 EXCEPCIONES

Toda solicitud de excepción de alguna política de seguridad informática debe ser solicitada a Secretaría Asuntos Administrativos y a la Dirección de Tecnologías de la Información y las Comunicaciones o a quien corresponda, con la debida justificación y documentación conforme la naturaleza de su cargo o dado por eventos no contemplados en esta Política de Seguridad Informática; previa evaluación del alcance y el impacto. La evaluación de la excepción puede requerir el apoyo de la Secretaría Jurídica.