Decreto Número (261)
Junio 30 de 2015

"POR LA CUAL SE ADOPTAN LAS POLITICAS DE SEGURIDAD INFORMÁTICA DE LA ALCALDÍA DE DOSQUEBRADAS - RISARALDA"

El alcalde Municipal de Dosquebradas – Risaralda, en uso de las facultades constitucionales, legales y reglamentarias, especialmente las contenidas en el Artículo 315° de la Constitución Política; la Ley 136 de 1994 Artículo 91°, Modificado por el Artículo 29° de la ley 1551 de 2012.

CONSIDERANDO:

1° Que la información de la Alcaldía de Dosquebradas es uno de los activos mas importantes para la entidad y por lo tanto se le debe dar un tratamiento seguro, con el fin de mantener la confidencialidad, integridad y disponibilidad de la misma.

2° Que la Constitución Política de Colombia establece varios principios esenciales relacionados con la función de los archivos en la vida social, tales como el derecho a la información, el acceso a los documentos públicos y el principio de la democracia participativa, que obligan a las entidades públicas a implementar sistemas de gestión de la Calidad.

3° Que el documento CONPES 3701 del 14 de julio de 2011, busca generar los "Lineamientos de política para ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país".

4° Que la Ley 1341 de 2009, considera: que es función del Estado intervenir en el sector de las TIC con el fin de promover condiciones de seguridad del servicio al usuario final, incentivar acciones preventivas y de seguridad informática y de redes para el respectivo sector. (Art. 4°, Numeral 11)

5° Que entre los componentes del Manual de Gobierno En Línea (GEL) contenido en el Decreto 1078 de 2015, Artículo 2.2.9.1.2.1, Numeral 4° dice: "Seguridad y privacidad de la información: ... proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada".

6° Que se debe establecer un modelo conceptual y operativo, así como una arquitectura tecnológica acorde con las políticas de gobierno electrónico internacionalmente aceptadas.

7° Que se debe garantizar el acceso a toda la información pública sin perjuicio de las restricciones de Ley.

8° Que, conforme a lo anterior, la Alcaldía de Dosquebradas, requiere la implementación de unas políticas de Seguridad Informática.

DECRETA:

ARTICULO PRIMERO: ADOPCION DE LAS POLITICAS DE SEGURIDAD INFORMÁTICA. Adoptar las Políticas de Seguridad Informática de la Alcaldía de Dosquebradas, contenido en el anexo en 11 folios, que hace parte integral del presente Decreto.

ARTICULO SEGUNDO: ALCANCE. Las disposiciones de las presentes Políticas se aplicarán a todas las dependencias y sujetos obligados de la Administración Central del Municipio de Dosquebradas.

ARTICULO TERCERO: VIGENCIA. El presente Decreto rige a partir del treinta (30) de Junio de dos mil quince (2015)

PUBLIQUESE, COMUNIQUESE Y CUMPLASE

JORGE DIEGO RAMOS CASTAÑO
Alcalde Municipal

JUAN CARLOS AGUDELO SANCHEZ
Director Administrativo

HUGO ALEJANDRO SALAZAR SALAZAR
Asesor externo

Proyectó: Serafín Saavedra Rivera – Técnico Administrativo G2

POLITICAS DE SEGURIDAD INFORMÁTICA

ALCALDIA DE DOSQUEBRADAS - RISARALDA

CONTENIDO

Proyectó: Serafin Saavedra Rivera – Técnico Administrativo G2

CAPITULO I

1. GENERALIDADES

La información de la Alcaldía de Dosquebradas es uno de los activos más importantes para la entidad, y por lo tanto se le debe dar un tratamiento seguro, bajo la supervisión de los Secretarios, Directores, Asesores o quien haga sus veces 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.

MARCO LEGAL:

Constitución Política de Colombia:

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

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".

Decreto 1078 de 2015: Objeto: "Definir los lineamientos, instrumentos y plazos de la Estrategia de Gobierno En Línea para garantizar el máximo

Proyectó: Serafín Saavedra Rivera – Técnico Administrativo 32

Avenida Simón Bolívar – Centro Administrativo Municipal CAM – Teléfono: (6) 3320523
sistemas@dosquebradas.gov.co código postal 661001

aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad".

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".

Documento Conpes 3701 de 2011: "Lineamientos de política para Ciberseguridad y Ciberdefensa".

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

Proyectó: Serafin Saavedra Rivera – Técnico Administrativo G2

Avenida Simón Bolívar – Centro Administrativo Municipal CAM – Teléfono: (6) 3320523
sistemas@dosquebradas.gov.co código postal 661001

CAPITULO II

2. CUENTAS DE USUARIO DE LOS SISTEMAS

2.1. 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, dominio, VPN, etc.).

2.2. 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).

2.3. Los usuarios deben establecer contraseñas que no sean fácilmente identificables.

2.4. 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).

2.5. 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.

2.6. Toda desvinculación de funcionarios de la entidad, deberá ser comunicada por el jefe del funcionario a La Secretaría General y de las TIC con el fin de cancelar los accesos a los sistemas de información y recuperar los activos informáticos asignados.

2.7. Las contraseñas de los usuarios administradores de las plataformas tecnológicas y sistemas de la compañía deberán ser salvaguardados bajo custodia del Profesional Especializado TIC o quien este delegue, en un archivo protegido a través de técnicas de cifrado de datos u otro mecanismo seguro.

Proyectó: Serafín Saavedra Rivera – Técnico Administrativo G2

Avenida Simón Bolívar – Centro Administrativo Municipal CAM – Teléfono: (6) 3320523
sistemas@dosquebradas.gov.co código postal 661001

CAPITULO III

3. CLASIFICACIÓN DE LA INFORMACIÓN

3.1. 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**". Sólo se podrá tener acceso a información clasificada como "**Publica Clasificada**" o "**Publica Reservada**" bajo previa aprobación del "sujeto obligado" de la información.

De acuerdo a la Ley 1712 de 2014 de Trasparencia, Articulo 6, 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.

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

3.3. El primer responsable de verificar que la Información cuente con controles adecuados que eviten su perdida, daño o divulgación no autorizada es el sujeto obligado de la Información.

3.4. 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

Avenida Simón Bolívar – Centro Administrativo Municipal CAM – Teléfono: (6) 3320523
sistemas@dosquebradas.gov.co código postal 661001

Avenida Simón Bolívar – Centro Administrativo Municipal CAM – Teléfono: (6) 3320523
sistemas@dosquebradas.gov.co código postal 661001

Autorizadas); e Integridad (la información no debe poder ser alterada o destruida de manera no autorizada para afectar la entidad).

CAPITULO IV

4. ACUERDOS DE CONFIDENCIALIDAD Y DERECHOS DE PROPIEDAD INTELECTUAL

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

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

CAPITULO V

5. SEGURIDAD DE LA RED INTERNA Y PERIMETRAL

5.1. 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 Profesional Especializado TIC.

5.2. 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.

5.3. 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 Profesional Especializado TIC.

5.4. Todas las redes inalámbricas existentes en la entidad deberán cumplir con los Estándares de Seguridad definidos por la Secretaria General y de las TIC.

Proyectó: Serafin Saavedra Rivera – Técnico Administrativo G2

CAPITULO VI

6. BUEN USO DE RECURSOS INFORMÁTICOS

6.1. 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.

6.2. 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.

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

6.4. No está permitida la instalación de ningún software adicional al aprobado por la Secretaria General a través del Profesional Especializado TIC.

6.5. El usuario es responsable de realizar las copias de seguridad requeridas para proteger la información almacenada en los equipos asignados, a través de las herramientas que Secretaria General y de las TIC provea.

6.6. Ningún usuario está autorizado para compartir información de su equipo a todos los usuarios de la red sin establecer restricciones.

CAPITULO VII

7. TRABAJO EXTERNO

7.1. 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.

Proyectó: Serafín Saavedra Rivera – Técnico Administrativo G2

7.2. La información Publica Clasificada o Publica Reservada de la entidad no puede ser copiada en medios externos con excepción de aquellas autorizadas por la Ley, en dispositivos asignados por la Secretaría General y de las TIC 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 compañía y estableciendo una contraseña fuerte.

CAPITULO VIII

8. FORMACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

8.1. Todos los funcionarios de la Alcaldía de Dosquebradas deben recibir capacitación sobre las Políticas de Seguridad de la Información definidas.

CAPITULO IX

9. MANTENIMIENTO Y CONSERVACION DE EQUIPOS Y REDES

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

9.2. Todos los funcionarios deberán mantener sus equipos de cómputos limpios y aseados. Cuando se requiera de mantenimiento especializado se debe solicitar al Profesional Especializado TIC o a quien éste designe.

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

9.4. 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.

Avenida Simón Bolívar – Centro Administrativo Municipal CAM – Teléfono: (6) 3320523
sistemas@dosquebradas.gov.co código postal 661001

CAPITULO X

10. SEGURIDAD EN LA REUTILIZACIÓN O ELIMINACIÓN DE EQUIPOS

10.1. 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.

10.2. 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)

CAPITULO XI

11. CORREO ELECTRONICO, INTERNET, WEB E INTRANET

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

11.2. 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.

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

11.4. La página WEB será administrada exclusivamente por el Profesional Especializado del área de la Secretaria General y de las TIC de y la publicación de información y contenidos, serán responsabilidad del sujeto obligado quien genera la información.

11.5. 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 del Profesional Especializado del área de la Secretaria General y de las TIC y la información y sus contenidos serán responsabilidad del sujeto obligado.

Proyectó: Serafin Saavedra Rivera – Técnico Administrativo G2

CAPITULO XII

12. ACCESO FÍSICO A ÁREAS SENSIBLES

12.1. 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 el Profesional Especializado del área de la Secretaria General y de las TIC.

CAPITULO XIII

13. USO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO DE INFORMACIÓN

13.1. 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"**). Sólo aquellos funcionarios con claras necesidades tendrán habilitados estos dispositivos con la previa autorización.

CAPITULO XIV

14. INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

14.1. El profesional Especializado del área TIC de la Secretaria General y de las TIC verificará el cumplimiento de las Políticas de Seguridad de la Información apoyado en las herramientas informáticas implementadas en la Alcaldía. Cuando se identifique un Incidente de Seguridad de la Información, éste será reportado al sujeto obligado de la Información.

14.2. 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

Proyectó: Serafín Saavedra Rivera – Técnico Administrativo G2

código de ética.

Elaboró:

SERAFÍN SAAVEDRA RIVERA
Técnico Administrativo G2

Visto Bueno:

HUGO ANDRES OROZCO RIOS
Profesional Especializado

Aprobó:

JUAN CARLOS AGUDELO SÁNCHEZ
Secretario General y de las TIC

Proyectó: Serafín Saavedra Rivera – Técnico Administrativo G2