RESOLUCION No. 033- 2022
(marzo 11 de 2022)

"POR MEDIO DE LA CUAL SE ACTUALIZA LA POLITICA DE SEGURIDAD DE LA INFORMACION DE LA CONTRALORIA MUNICIPAL DE DOSQUEBRADAS"

La Contralora Municipal (E) de Dosquebradas, en uso de sus atribuciones constitucionales y de Ley, conferidas por los articulo 267 y 272, y ley 909 de 2004, decreto 1083 de 2015,

C O N S I D E R A N D O:

Que la Constitución Política de Colombia en el artículo 15, consagra que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidad públicas y privadas.

Que así mismo, el artículo 209 superior, establece que la administración Pública, en todos sus órdenes, tendrá un control interno, el cual ejercerá en los términos que señala la Ley. El artículo 269 ordena a las autoridades de las entidades públicas la obligación de diseñar y aplicar, según su naturaleza de sus funciones métodos y procedimientos de control interno.

Que el Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.3, define a la seguridad de la información como un principio de la Política de Gobierno Digital, de igual manera, en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores trasversales los cuales son elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Que el Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 (Decreto Único reglamentario del Sector de Función Pública, adoptó el Modelo Integrado de Planeación y Gestión MIPG, definiéndolo en su artículo 2.2.22.3.2 como *"....es un marco de referencia para dirigir , planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que tiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio"*

Que el artículo 2.2.22.2.1 del Decreto 1083 de 2015, sustituido por el artículo 1º del Decreto 1499 de 2017, regula las políticas de Gestión y

Desempeño Institucional, entre las que se encuentran las de "*11 Gobierno Digital, antes Gobierno en Línea" y "12 Seguridad Digital"*

Que es responsabilidad del Comité Institucional de Gestión y Desempeño de la **Contraloría Municipal de Dosquebradas** "*Aprobar y apoyar la implementación de los planes de continuidad del negocio que se establezcan con el fin de mitigar los riesgos asociados a la interrupción de la operación", y por tanto es necesario adoptar las acciones pertinentes para el efecto.*

Que, conforme a los cambios normativos y madurez en el Sistema de Gestión de Seguridad de la Información, fue necesaria la revisión y ajuste a la política de Seguridad de la Información de la **Contraloría Municipal de Dosquebradas**, contenida en la Resolución No. 012 (enero 20 de 2022), "POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE DESARROLLO TECNOLOGICO PARA LA VIGENCIA 2022".

Que dado lo anterior, se hace necesario adoptar mediante acto administrativo la Política de Seguridad de la Información, así como definir los lineamientos para su implementación y gestión

En mérito de lo expuesto:

RESUELVE

ARTICULO PRIMERO: **Objeto:** La presente Resolución tiene como objeto ajustar la Política de Seguridad de la Información y definir lineamientos frente a su implementación y gestión

ARTICULO SEGUNDO: **Adoptar:** Las políticas, normas y procedimientos de seguridad de la información, como una decisión estratégica de la **Contraloría Municipal de Dosquebradas**, con el fin de definir el MPSI, establecer un modelo de seguridad y privacidad de la información.

ARTICULO TERCERO: **Aprobar el anexo técnico,** que hace parte integral de este acto administrativo, el cual contiene los lineamientos que permiten proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de la información de la **Contraloría Municipal de Dosquebradas**.

ARTICULO CUARTO: **Encargar** a la Dirección Operativa Administrativa y Financiera de la **Contraloría Municipal de Dosquebradas**,

como responsable de la orientación y ajustes de la administración de la Seguridad de los activos de información, proveer las bases de datos para el seguimiento y monitoreo en la entidad, asegurando constantemente la confidencialidad, integridad y disponibilidad de la información.

ARTICULO QUINTO: **Determinar la responsabilidad de los funcionarios y Contratista, frente al uso de los Recursos Tecnológicos:** todos los funcionarios y contratistas que hagan uso de los bienes o servicios tecnológicos y de los los activos de la información pertenecientes a la **Contraloría Municipal de Dosquebradas**, y en cumplimiento de disposiciones legales relacionados con la seguridad de la información, con la responsabilidad de cumplir las políticas establecidas para su uso adecuado, entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación y por ende el cumplimiento de la misión institucional.

ARTICULO SEXTO: **Revisión y Actualización:** La política deberá ser revisada mínimo una vez al año o cuando ocurran cambios significativos

ARTICULO SEPTIMO: **Vigencia** La presente resolución rige a partir de la fecha de su expedición y deroga todas las disposiciones que le sean contrarias.

ARTICULO OCTAVO: PUBLIQUESE, COMUNIQUESE Y CUMPLASE

Dada en Dosquebradas, Risaralda a los once (11) días del mes de marzo de 2022

MARGARITA MARIA GALLEGO GUTIERREZ
Contralora Municipal (E)

Proyecto: María del Pilar Loaiza Hincapie (DOT) (e)

POLÍTICA GENERAL

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la **Contraloría Municipal de Dosquebradas** con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La Contraloría Municipal de Dosquebradas, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la **Contraloría Municipal de Dosquebradas.**
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

- Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la **Contraloría Municipal de Dosquebradas** y la ciudadanía en general.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política. A continuación, se establecen las políticas de seguridad que soportan el MSPI de **La Contraloría Municipal de Dosquebradas**:

- La **Contraloría Municipal de Dosquebradas** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- **La Contraloría Municipal de Dosquebradas** protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de estos.

- **La Contraloría Municipal de Dosquebradas** protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- **La Contraloría Municipal de Dosquebradas** protegerá su información de las amenazas originadas por parte del personal.
- **La Contraloría Municipal de Dosquebradas** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- **La Contraloría Municipal de Dosquebradas** controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- **La Contraloría Municipal de Dosquebradas** implementará control de acceso a la información, sistemas y recursos de red.
- **La Contraloría Municipal de Dosquebradas** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- **La Contraloría Municipal de Dosquebradas** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- **La Contraloría Municipal de Dosquebradas** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- **La Contraloría Municipal de Dosquebradas** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

CONTRALORIA MUNICIPAL DE DOSQUEBRADAS

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

2022

1. INTRODUCCION.

La adopción de políticas, normas y procedimientos de seguridad de la información obedece a una decisión estratégica de la dirección operativa administrativa y financiera de la **Contraloría Municipal de Dosquebradas**, con el fin de definir el MPSI, a través del análisis, diseño e implementación de los objetivos, requisitos de seguridad, procesos, procedimientos, planes, políticas, controles con formatos, la tecnología y estructura de esta.

En la actualidad la información para la **Contraloría Municipal de Dosquebradas** se reconoce como un activo supremamente valioso y en la medida que los sistemas de información apoyan cada vez más los procesos misionales y de apoyo, y debido a lo anterior se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de la misma.

Se ha definido que las políticas de seguridad de la información deben identificar responsabilidades y establecer los objetivos para una protección apropiada de los activos de información de la entidad, contando además con manuales para usuarios finales. La implementación de las políticas busca reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, destruya o use en forma indebida la información de la entidad.

Al mismo tiempo las políticas habilitan a la dirección operativa administrativa y financiera como responsables de dictar los lineamientos de la gestión de seguridad de la información, y para orientar y mejorar la administración de seguridad de los activos de información. Finalmente, también contempla el proveer las bases para el seguimiento y monitoreo en la entidad. La **Contraloría Municipal de Dosquebradas**, desde sus directivas pretende mantener un esquema de seguridad que permita asegurar constantemente la confidencialidad, integridad y disponibilidad de la información, siendo esta, su activo más valioso.

Para ello adopta, establece, implementa, opera, verifica y mejora un Sistema de Gestión de Seguridad de la Informacion (MSPI). Con base en lo anterior se debe integrar a todo el personal de la entidad para que, conozca, participe y cumpla los lineamientos, políticas, procedimientos y demás directrices estipuladas en el MSPI.

2. OBJETIVOS.

2.1 Objetivo General

Establecer los lineamientos que permitan proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la **Contraloría Municipal de Dosquebradas**, teniendo en cuenta los procesos, la operación, los objetivos de negocio y los requisitos legales vigentes en la entidad.

Contenido

2.2 Objetivos específicos

- Definir la política de seguridad y privacidad de la información de la **Contraloría Municipal de Dosquebradas**.
- Definir los lineamientos a ser considerados para disertar e implementar el modelo de seguridad y privacidad de la información, alineado con las necesidades, los procesos, los objetivos y la operación de la **Contraloría Municipal de Dosquebradas**.
- Dar conformidad y cumplimiento a las leyes, regulaciones y normativas que se aplican a la **Contraloría Municipal de Dosquebradas** en el desarrollo de su misión.
- Proteger los activos de información de la **Contraloría Municipal de Dosquebradas**.
- Mantener un sistema de políticas, manuales, procedimientos y estándares actualizados, a efectos de asegurar su vigencia y un nivel de eficacia, que permitan minimizar el nivel de riesgo de los activos de información de la **Contraloría Municipal de Dosquebradas**.
- Fortalecer la cultura de seguridad de la información en funcionarios, terceros y clientes de **Contraloría Municipal de Dosquebradas**, mediante la definición de una estrategia de uso y apropiación de la política.
- Garantizar la continuidad de negocio frente a la materialización de incidentes de seguridad basados en la norma ISO 27035. (Gestión de incidentes de seguridad de la información)
- Definir una estrategia de continuidad de los procesos de la entidad frente a incidentes de seguridad de la Informacion.

3. ALCANCE.

La política de Seguridad de la Informacion es aplicable en todo el ciclo de vida de los activos de información de la **Contraloría Municipal de Dosquebradas**, incluyendo creación, distribución, almacenamiento y destrucción. De igual forma para todos los funcionarios, contratistas y terceros que desempeñen alguna labor en la entidad. El alcance abarca desde el enunciado de la política, pasando por los lineamientos para la implementación del Sistema Seguridad y Privacidad de la Informacion, la matriz de riesgo, la definición de los indicadores para el monitoreo de cumplimiento de la política hasta la definición de una estrategia para la adopción de la política en la entidad.

4. MARCO NORMATIVO Y REGULATORIO.

La **Contraloría Municipal de Dosquebradas**, como entidad pública, al igual que cualquier organismo del estado, se encuentra cubierta por un marco normativo y regulatorio en todo lo relacionado con la seguridad de la información, como también un marco de referencia de las mejores prácticas para el desarrollo e implementación del Sistema de Gestión de Seguridad de la Informacion.

Se tiene en cuenta especial mente la nueva Estrategia de Gobierno Digital, que se evidencia en el Decreto Único Reglamentario del Sector de Tecnologías de

la Informacion y las Comunicaciones 1078 de 2015, comprende cuatro grandes propósitos: lograr que los ciudadanos cuenten con servicios en línea de muy alta calidad, impulsar el empoderamiento y la colaboración de los ciudadanos con el Gobierno, encontrar diferentes formas para que la gestión en las entidades públicas sea optima gracias al uso estratégico de la tecnología y garantizar la seguridad y la privacidad de la información.

A continuación, se relacionan las demás normas, leyes, decretos y resoluciones que aplican para el establecimiento, implementación y operación del MSPI en la **Contraloría Municipal de Dosquebradas**:

- NTC-ISOIIEC 27001- 27002:2013
- Decreto 2693 de 2012 MinTic
- Decreto 1008 de 2018 MinTic.
- Decreto 1414 de 2017 de MinTic.
- Ley 1712 de 2014
- Ley 1273 de 2009
- Decreto 1078 de 2015 MinTic
- Ley 1581 de 2012.
- Decreto 415 de 2016 MinTic
- Decreto 1377 de 2013
- Ley 1266 de 2008

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACÓN.

5.1 POLÍTICA GENERAL

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la **Contraloría Municipal de Dosquebradas** con respecto a la protección de los activos de información, que soportan los procesos de la Entidad y apoyan la implementación el modelo de seguridad y privacidad de la información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La Contraloría Municipal de Dosquebradas, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el modelo de seguridad y privacidad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la **Contraloría Municipal de Dosquebradas.**
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

- Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la **Contraloría Municipal de Dosquebradas** y la ciudadanía en general.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento de la política. A continuación, se establecen las 12 políticas de seguridad que soportan el MPSI en l**a Contraloría Municipal de Dosquebradas**:

- La **Contraloría Municipal de Dosquebradas** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- **La Contraloría Municipal de Dosquebradas** protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de estos.
- **La Contraloría Municipal de Dosquebradas** protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- **La Contraloría Municipal de Dosquebradas** protegerá su información de las amenazas originadas por parte del personal.
- **La Contraloría Municipal de Dosquebradas** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- **La Contraloría Municipal de Dosquebradas** controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- **La Contraloría Municipal de Dosquebradas** implementará control de acceso a la información, sistemas y recursos de red.
- **La Contraloría Municipal de Dosquebradas** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- **La Contraloría Municipal de Dosquebradas** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- **La Contraloría Municipal de Dosquebradas** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

- **La Contraloría Municipal de Dosquebradas** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

Esta política se aplica a todos los funcionarios, contratistas y terceros de la entidad sin excepción, en donde cada uno de los cuales cumple un rol en la administración de la seguridad de la información. Todos funcionarios, contratistas y terceros de la entidad son responsables de mantener un ambiente seguro, en tanto que la dirección operativa administrativa y financiera debe monitorear el cumplimiento de las políticas de seguridad definidas y realizar las actualizaciones que sean necesarias.

Las políticas deben ser revisadas mínima una vez, por el periodo del Contralor o cuando se produzca un cambio relevante en la operación que implique realizar ajustes al producto de los cambios en el entorno tecnológico y/o de las necesidades de la operación.

6.1 Apoyo de la dirección.

El Despacho y las Directivas de la **Contraloría Municipal de Dosquebradas** deben apoyar activamente la seguridad de la información dentro de la entidad, definir un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información. Este compromiso se verá reflejado a través de:

6.1.1 Se debe crear al interior de la entidad un comité de seguridad de la información o uno quien haga sus veces, que sea interdisciplinario y formalizado por una resolución interna

6.1.2 Dirección operativa de la **Contraloría Municipal de Dosquebradas** debe mantener dentro de sus colaboradores un funcionario o contratista con el perfil de Oficial de Seguridad de la Informacion, quien será el encargado de todo lo relacionado con la seguridad de la información y cuyas funciones estarán caracterizadas y definidas en la presente política.

6.1.3 Se debe velar por el cumplimiento de las políticas de seguridad de la información, comprometerse para que los funcionarios a su cargo conozcan y apliquen las políticas de seguridad de la información.

6.1.4 La dirección de la **Contraloría Municipal de Dosquebradas** o el Comité de seguridad de la Informacion (o quien haga sus veces), debe apoyar, facilitar y mantener cuando se requiera relaciones con empresas, entidades u organismos que presten asesoría especializada en seguridad de la información.

Se deben establecer tres niveles diferentes de gestión de la seguridad de la información, en la participacion de la definición y aplicación del MSPI:

- Estratégico: - Dirigir y proveer: Definir los grandes lineamientos directivos o gerenciales para la seguridad de la información y la política global del MSPI, coordinar y aprobar los recursos.

- Táctica: - Implementar y optimizar: Diseñar e Implementar el MSPI, establecer objetivos concretos / específicos, gestionar los recursos.

- Operacional: - Ejecutar y reportar: Alcanzar los objetivos específicos mediante procesos técnicos.

6.2 Las direcciones de la Contraloría Municipal de Dosquebradas

Todas las direcciones de la entidad deben tener en cuenta y cumplir los siguientes lineamientos:

6.2.1 Toda adquisición e implementación de una solución o plataforma tecnológica (hardware o software), debe contar con el visto bueno, concepto técnico y acompañamiento de la dirección operativa administrativa y financiera, en donde se evalúen los aspectos de viabilidad técnica al momento previo de la realización de la liberación de pedido, compatibilidad, capacidad, integridad y disponibilidad, tanto desde la óptica de infraestructura de TIC, como el de seguridad de la información.

6.2.2 Todo requerimiento, incidente, problema o cambio debe ser reportado y tramitado por medio de la dirección operativa administrativa y financiera, como único medio valido y autorizado para estos fines.

6.2.3 Incluir y tener en cuenta los lineamientos y políticas de Seguridad de la información en la gestión de la contratación con terceros, proveedores y contratistas, así como en la gestión de proyectos, independientemente del tipo de proyecto.

6.2.4 Cumplir y apoyar el cumplimiento de todas las políticas, normas, manuales y procedimientos de seguridad de la información.

6.3. Funcionarios y Contratistas de la Contraloría Municipal de Dosquebradas

Los usuarios de la información (funcionarios - contratistas - proveedores - terceros) y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer y cumplir la Política de Seguridad de la Informacion vigente. Los funcionarios - contratistas - proveedores - terceros de la **Contraloría Municipal de Dosquebradas**, deben.

6.3.1 Conocer, comprender y aplicar la Política de Seguridad de la información de la **Contraloría Municipal de Dosquebradas** en los procedimientos que apliquen a su trabajo

6.3.2 Llevar a cabo su trabajo, asegurándose de que sus acciones no producen ninguna infracción de seguridad de la información.

6.3.3 Comunicar las incidencias de seguridad de la información que detecte a la dirección operativa administrativa y financiera.

6.3.4 Hacer uso de las mejores prácticas definidas en la entidad para todos los temas relacionados con la seguridad de la información.

6.3.5 Cumplir con el acuerdo de confidencialidad firmado con la entidad, conforme a lo señalado en la Resolución 026 de 2022

6.3.6 Reportar a la dirección operativa administrativa y financiera cualquier anormalidad que atente contra la seguridad de la información en la Entidad.

6 .4 Responsables de la información.

El propietario de un activo de información, entendiéndose como tal, aquel que es el responsable de dicho activo, tendrá las siguientes responsabilidades:

6.4.1. Definir si el activo de información está afectado por la Ley 1581 de 2012 de Protección de Datos y aplicarle en su caso, los procedimientos correspondientes.

6.4.2. Definir quienes pueden tener acceso a la información, como y cuando, de acuerdo con la clasificación interna de la información y la función a desempeña. (Ley 1581 de 2012)

6.4.3. Implementar las medidas de seguridad de la información necesarias en su área para evitar fraudes, robos o interrupción en los servicios.

6.4.4. En los casos que aplique, asegurarse de que el personal; funcionarios, contratistas y proveedores tienen cláusulas de confidencialidad en sus contratos y son conscientes de sus responsabilidades.

6.4.5. Conocer, comprender y aplicar la Política de Seguridad de la información de la **Contraloría Municipal de Dosquebradas** en los procedimientos que apliquen a su trabajo.

6.5 Revisión del MPSI

El despacho y las Direcciones, deberán revisar el Modelo de privacidad y seguridad de la Información (MPSI) de La **Contraloría Municipal de Dosquebradas** a intervalos planificados, (por lo menos una por periodo), para asegurar su conveniencia, suficiencia y eficacia. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del MSPI, incluidos la política de seguridad y los objetivos de seguridad. Los resultados de las revisiones se deben documentar

claramente y se deben llevar registros. Esta revisión cumplirá con los lineamientos establecidos en el procedimiento de revisión del Sistema Integrado de Gestión.

De la misma manera, las políticas de seguridad de la información, normas, procedimientos, estándares, controles, formatos y procedimientos, deben ser revisados y actualizados sistemáticamente, de forma periódica y planificada (mínimo una vez por periodo o cada vez que ocurra un cambio sustancial en los activos de información), se debe realizar por un organismo, empresa o consultor externo especializado, en cuyo caso debe seguir los lineamientos de la norma NTC-ISOIIEC 27001 :2013 y debe ser realizada por alguien con las credenciales de AUDITOR LIDER (Lead Auditor) 27001 vigentes o Auditor CISA preferiblemente.

7. GESTION DE ACTIVOS

Esta política nace como un instrumento de la institución para sensibilizar a los diferentes usuarios que hacen uso de los sistemas de información, con el fin de describirles la protección y el funcionamiento para la utilización adecuada y reconociéndolo como un canal de información que presta servicios integrales, confidenciales y direccionándolos a la prestación de un servicio eficaz.

El propósito de esta política es establecer límites que resguarden la información de ser liberada (deliberada o no deliberadamente) a las personas erradas. En la **Contraloría Municipal de Dosquebradas** la Información es un activo esencial para la prestación del servicio y la toma de decisiones, por lo cual existe un deber manifiesto de salvaguardar la propiedad más relevante como estrategia orientada a la continuación de la institución, la administración de peligros y el fortalecimiento de la cultura de seguridad. Dentro de esta política se establecerá la protección de los activos de la información que cumple con la visión institucional:

1. Los activos de información de la **Contraloría Municipal de Dosquebradas**, serán identificados, clasificados y socializados, con el fin de instituir los elementos de protección necesarios.
2. **La Contraloría Municipal de Dosquebradas** a través de la dirección operativa administrativa y financiera, definirá e implementará controles para proteger la información y garanticen la disponibilidad solicitada por los usuarios de los servicios ofrecidos por la Institución.
3. Todos los funcionarios de la institución incluyendo los contratistas, serán responsables de proteger la información a la cual tienen acceso para evitar riesgos (pérdida, alteración, uso indebido o destrucción).
4. Se programarán auditorias y controles pertinentes a los sistemas de información existentes.
5. Solo se permitirá software que se haya adquirido legalmente y el software libre que brinde seguridad y soporte.
6. Los funcionarios y contratistas, como responsabilidad sobre la seguridad de la información, deberán comunicar los riesgos que identifique.
7. El incumplimiento de las políticas será notificadas, reconocidas y monitoreadas.

8. **La Contraloría Municipal de Dosquebradas** en cabeza del comité de gestión y desempeño y la dirección operativa administrativa y financiera, elaborara un plan de continuidad de las actividades de la Institución ante eventos que puedan ocurrir.

7.1 Política de seguridad de red.

7.1.1. Servidor

Para garantizar la seguridad de la información en la entidad, debe propender porque los servidores manejen un volumen de gestión alto y estén en sitios especializados que brinden servicio de almacenamientos, despliegue de aplicativos y para la gestión interna administrativa y financiera, es recomendable que los servidores este en un sitio institucional ideal. En este sentido, los servidores (Web, BD, Aplicaciones, entre otros.), de la entidad están respaldados en la navegación por firewall para seguridad perimetral, el mantenimiento físico y lógico especial de estos equipos y las políticas de navegación específicas que se establezcan. Otros controles que se presentes son las restricciones al espacio físico donde están ubicados los equipos servidores (aparte de los equipos de usuarios) para evitar el intento de acceso a la parte lógica.

7.1.2 Protección física y digital de la información

Para evitar la vulnerabilidad en las aplicaciones locales y de internet en los equipos de los usuarios, se deben tomar medidas de acuerdo al tipo de software, implementando otra clase de protecciones; como el antivirus corporativo, antivirus de red, administración de los usuarios donde se determine el acceso y las restricciones pertinentes, entre otras actividades que permitan mitigar el posible riesgo.

En este apartado se define lineamientos que deberán adoptarse al interior de la institución para la protección de la información, tanto física como digital y con acceso a través de los sistemas de cómputo, estos lineamientos deberán ser seguidos por todos y cada una de las áreas implicadas en estas actividades.

Para **la Contraloría Municipal de Dosquebradas**, es de vital importancia proteger información sensible, evitando que sea conocida por personas diferentes a aquellas que la requieren o que sea publicada de manera indistinta. Por tanto, los usuarios deberán cumplir lo siguiente:

- La información de la institución deberá mantenerse disponible a las personas autorizadas para ello en el momento en que se necesite, lo que hace que la información sensible se pueda encontrar en el puesto de trabajo de cada empleado durante su jornada, sin que esto deba ser entendido como admitir momentos en que la información NO esté debidamente protegida. A pesar de que los niveles de protección y clasificación establecidos para la información de la institución son mantenidos en todo momento el usuario con acceso a estos sistemas de información deberán estar pendiente que solo el sea el responsable de acceder al sistema de información que por su trabajo deba acceder.
- Los usuarios dueños de la información son responsables, mientras tengan la información bajo su control, de mantener los niveles de protección y

clasificación establecidos para la misma en todo momento, haciendo uso adecuado de los recursos a su disposición.

- Es responsabilidad de los usuarios el identificar riesgos relacionados al disponer de la información en su puesto de trabajo e iniciar las acciones para mitigarlos.
- Durante la jornada laboral, los usuarios deben propender por tener el Escritorio Limpio, los sistemas de información y elementos de procesamiento deberán ser adecuadamente protegidos, teniendo presente que se debe al menos guardar documentos confidenciales o elementos de almacenamiento de información (CDS, DVDs, Memorias USB, Discos móviles, asistentes personales, portátiles) en los cajones bajo llave, en todo momento que no los esté utilizando.
- Es responsabilidad de cada usuario la protección de los sistemas de información a su cargo, por lo que debe asegurar físicamente el computador portátil con cables de seguridad en todo momento para evitar robos o si es equipo de escritorio tratar de asegurar el hardware y para el software colocar clave de acceso.
- Es responsabilidad de cada usuario la protección de la información a cargo, por lo que debe mantener presente NO publicar o dejar a la vista, documentos o datos confidenciales, delicados, confidenciales, por ejemplo:
    - Nombre de Usuario y Password
    - Direcciones IP
    - Contratos
    - Números de Cuenta
    - Listas de Clientes
    - Datos de funcionarios
    - Cualquier cosa que no desea publicar
    - Dejar el Escritorio Limpio después de la jornada laboral y lo confidencial Bajo llave.
    - Los usuarios de la **Contraloría Municipal de Dosquebradas** deberán tomarse el tiempo necesario antes de abandonar la oficina para recoger y asegurar el material confidencial. (Portátiles, PDAs, tables, Memorias USB, entre otros.).

Cada usuario de la entidad para mantener su computador bajo control, deberá bloquear la sesión al alejarse de su computador, aunque sea por poco tiempo, minimizando el tiempo que el equipo quedaría sin control ya que cualquier ausencia puede extenderse.

7.1.3 Protección contra software maligno

La intención en este punto es mencionar los controles que permiten minimizar el riesgo generado por el acceso a Internet y a redes públicas, el intercambio de medios de almacenamiento removibles, el intercambio de información con instituciones externas, entre otras, los cuales exponen los sistemas de la **Contraloría Municipal de Dosquebradas** a la propagación interna y externa de software con código malicioso o nocivo, comprometiendo directamente la integridad, la disponibilidad y la confidencialidad de la información procesada por cada uno de los componentes de la red.

- Cualquier usuario que sospeche de una infección por un virus debe llamar la persona encargada de sistemas para ser guiado con instrucciones precisas en el procedimiento de eliminación del virus del computador.
- Los usuarios **No** deben transferir (bajar) software desde cualquier sistema que se encuentra por fuera de la red de **la Contraloría Municipal de Dosquebradas**.
- Los usuarios **No** deben utilizar software obtenido externamente desde Internet o de una persona u organización diferente a los distribuidores confiables o conocidos, a menos que el software haya sido examinado en busca de código malicioso y que haya sido aprobado por el encargado de sistemas.
- Antes de ser descomprimido, todo software transferido desde sistemas externos de **la Contraloría Municipal de Dosquebradas** debe ser analizado con un sistema antivirus aprobado.
- Antes que cualquier archivo sea restaurado en un computador de la institución, desde un medio de almacenamiento de respaldo, éste debe ser analizado con un sistema antivirus.
- Los usuarios intencionalmente **NO** deben escribir, generar, compilar, copiar, almacenar, propagar, ejecutar o intentar introducir cualquier código de computador diseñado para auto replicarse, deteriorar o que dificulte el desempeño de cualquier sistema de la entidad.

7.1.4 Protección durante la navegación en internet

Esta política expresa los controles que permiten minimizar el riesgo generado por el acceso a Internet y a redes públicas, el intercambio de medios de almacenamiento móviles, el intercambio de información con instituciones externas, entre otros, los cuales dejan en riesgo los sistemas de la **Contraloría Municipal de Dosquebradas** a propagación interna y externa de software con código malicioso o nocivo, comprometiendo directamente la integridad, la disponibilidad y la confidencialidad de la información procesada por cada uno de los componentes de la red. **La Contraloría Municipal de Dosquebradas** con el objetivo de facilitar la realización de labores diarias y administrativas brinda acceso a Internet para navegación a los funcionarios de todo tipo, de planta y contratistas, los cuales se ampararán en las políticas y formas de actuación expuestos en este documento.

Por lo tanto, la dirección operativa administrativa elaborará comunicaciones digitales y escritas para toda la comunidad sobre la navegación en la Web para garantizar que estén informados sobre los peligros de descargar archivos de Internet (el software espía, los troyanos y los atacantes externos), acceder a sitios desconocidos o de baja confianza y aceptar los mensajes sobre instalación de software que brinde el navegador. La **Contraloría Municipal de Dosquebradas** buscará garantizar de manera técnica que se controle el acceso a sitios que puedan afectar la productividad de la institución, la seguridad de su información o del recurso humano.

- Los usuarios deberán abstenerse de visitar espacios en la Web restringidos por la entidad, o sitios que afecten la productividad del dia.
- Se deberá evitar el acceso desde el espacio institucional a sitios relacionados con la pornografía y fundamentalmente si éste involucra a menores de edad. Igualmente, se prohibió la descarga y uso de software malicioso o documentos que brinden información sobre cómo atentar contra la seguridad de la información institucional.

- Los funcionarios deberán abstenerse de brindar cualquier tipo de información de la institución en sitios no autorizados o que no cuenten con mecanismos de seguridad que garanticen la confidencialidad de la información en tránsito.
- Los funcionarios de la entidad **No** deben comprar bienes o servicios a través de Internet a nombre la **Contraloría Municipal de Dosquebradas**, a menos que exista una aprobación previa de las directivas pertinentes.
- Los usuarios, deben evitar descargar y/o emplear archivos de imagen, sonido o similares que puedan estar protegidos por derechos de autor de terceros sin la previa autorización de estos.
- Los usuarios no deben instalar software en sus estaciones de trabajo o en otras máquinas, incluso si este software es libre o no licenciado; toda instalación de software debe hacerla un técnico autorizado, luego de la debida verificación y la autorización previa de la Dirección operativa administrativa y financiera.
- Los usuarios están conscientes de que toda la información (incluida la de navegación) que transite en la institución por ser para la labor diaria es propiedad de la misma y por ende puede ser monitoreada con objetivos de administración, seguridad o auditoría por personal autorizado de la institución, si existen excepciones las establecerá el comité de seguridad y la Dirección.
- Los usuarios de los sistemas de navegación son conscientes de que estos, solamente deben ser utilizados para propósitos lícitos y en cumplimiento de las funciones específicas de su cargo, ya que toda actividad de navegación puede ser registrada por la **Contraloría Municipal de Dosquebradas**, quien podrá revelar cualquier acceso cuando una autoridad judicial así lo requiera.
- El personal de la **Contraloría Municipal de Dosquebradas** no debe utilizar el sistema de navegación para participar en grupos de discusión en Internet, listas de Correo, chats o cualquier otro foro público, a menos que su participación sea meramente con fines institucionales.
- **La Contraloría Municipal de Dosquebradas** facilita el acceso al uso de medios electrónicos para comercio electrónico como el pago de facturas, transacciones bancarias de sus funcionarios y lectura de correos personales que tengan acceso vía web, pero no asume ninguna responsabilidad por estas, ni recomienda el uso. Si el usuario hace uso de estos servicios de todas maneras asume que puede ser monitoreada toda la información que de este uso se derive como si fuese de la institución misma.

7.2 Política de seguridad de equipos.

7.2.1. Inventario de equipos.

Los equipos de cómputo de la entidad son los activos indispensables para la interacción tecnológica en la **Contraloría Municipal de Dosquebradas** y para el control general debe relacionar los siguientes registros:

- Usuario responsable del equipo.
- Código de los equipos asignado por la oficina de recursos físicos.
- Dirección IP.
- Confirmación hoja de vida
- Descripción general de las características técnicas del equipo (CPU).

- Marca
- Licencia Sistemas Operativo.
- Licencia herramienta ofimática.
- Fecha de adquisición.
- Observaciones generales

Actividades relacionadas con el registro de equipos:
- Cada que ingrese un equipo nuevo debe registrarse en el inventario.
- Cada que el equipo cambie de usuario debe actualizarse el inventario.
- Anualmente elaborar estadística de los datos registrados:
    - Cantidad de equipos por sistema operativo.
        - Cantidad de equipos por licenciados y no licenciados

7.2.2 Mantenimiento preventivo de equipos.

- Elaborar el cronograma anual para la programación del mantenimiento preventivo de los equipos de cómputo.
- De acuerdo con el cronograma, planear semestralmente la realización del mantenimiento preventivo a equipos de cómputo institucionales y notificar por escrito a cada usuario responsable del equipo de cómputo con anticipación.
- Llevar el control del mantenimiento preventivo programado semestralmente.
- Elaborar informe mensual del mantenimiento programado realizado – indicador de este servicio.
- Elaborar informe técnico por insolencia de un equipo para el servicio, por daños o fallas graves.
- Elaborar el registro de equipos y parte para baja por insolencia de un equipo para el servicio, por daños o fallas graves.
- Antes de la ejecución del mantenimiento preventivo, explicar al usuario como elaborar la copia de seguridad de la información de los equipos en responsabilidad.
- Brindar soporte al usuario en el manejo de software legal en el equipo (sistema operativo y herramientas ofimáticas).
- Al entregar el equipo con el mantenimiento preventivo programado, solicitarle al usuario la verificación del funcionamiento general del equipo, así como de la información.

7.2.3. Seguridad de los equipos:

Protección contravirus. Para la instalación de software antivirus informático, se debe:
- Verificar la capacidad de los equipos de cómputo, antes de la instalación.
- Realizar pruebas de funcionamiento una vez instalado.

7.2.4. Daño de equipos
- El equipo de cómputo o cualquier recurso tecnológico que sufra algún daño por maltrato, descuido o negligencia por parte del usuario comprobada, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado.

7.2.5. Protección y ubicación de los equipos de cómputo.

- 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 de la dirección operativa administrativa y financiera.
- El equipo de cómputo asignado deberá ser para uso exclusivo de las funciones asignadas al usuario de la **Contraloría Municipal de Dosquebradas**.
- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas entre otras instaladas y autorizadas en los equipos que utilizan, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos, a menos que sea en botellas de plástico.
- Se debe mantener el equipo informático en un entorno limpio y sin humedad.
- El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos. Exclusivamente el personal autorizado de la **Contraloría Municipal de Dosquebradas** podrá llevar a cabo los servicios y reparaciones a los equipos de cómputo, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.
- Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a mantenimiento o reparación y borrar aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de mantenimiento o reparación, solicitando la asesoría del soporte técnico de la persona encargada de sistemas.
- El usuario deberá dar aviso de inmediato a la dirección y la dirección operativa a la que pertenezca en caso de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su responsabilidad.

7.3 Software

7.3.1. Plan de respaldo y recuperación.

El respaldo y recuperación de la información que se maneja en la labor que se desempeña en la entidad es de vital importancia, por lo cual para la **Contraloría Municipal de Dosquebradas** es fundamental para garantizar la continuidad del procesamiento de los datos, con la mínima dificultad posible ante una eventual alteración no deseada. Para determinar cuándo hacer un respaldo y cuando recuperarlo debemos saber:

¿Qué es respaldo?
Es la obtención de una copia de la información, de los datos, de los documentos que manejamos en diferentes medios (magnéticos o en la nube), de tal forma que esta copia posibilite en un futuro la restauración o recuperación, estos respaldos deben realizarse con frecuencia establecida y para asegurar la validez, debe verificarse una vez se realice.

¿Qué es recuperación?

Es restablecer la información copiada para volverla al estado de aplicación o uso. Esta tarea se realiza esporádicamente, siempre y cuando se requiera, de igual manera se hace parcial o total. La Dirección Operativa Administrativa y Financiera realiza respaldo de la información que manejan los usuarios en sus computadores al momento del mantenimiento preventivo programado y se le entrega al usuario, quien deberá verificarla y entregar una copia al archivo central. La persona encargada del manejo de los Sistemas o quien haga sus veces es la encargada de realizar el respaldo de las bases de datos de los sistemas de información a los que tiene acceso directamente y solicitar a los que no tiene acceso.

7.3.2. Protección y respaldo de la información.

El propósito es mostrar el estado actual de protección de la información en la entidad y plantear estrategias para proteger y facilitar su utilización de acuerdo con las necesidades de prolongación trazadas a nivel de los procesos. En este documento se definen los parámetros que deberán seguirse al interior de la institución para el almacenamiento y recuperación de corto y largo plazo, así como de la recuperación de la información conservada a nivel de medios de almacenamiento para responder a los requerimientos de los procesos de la entidad. Estos parámetros deberán ser atendidos por los diferentes empleados que hacen parte de la **Contraloría Municipal de Dosquebradas**. Para la Institución el mayor activo es la información, por lo cual se deben crear procedimientos que garanticen un apropiado uso durante el ciclo de vida de la información, principalmente para los asuntos que requieren conservar la disponibilidad de esta, se deberá preservar la seguridad de la información dando cumplimiento a los principios de seguridad de la información.

- La información de la institución deberá mantenerse disponible a las personas autorizadas para ello en el momento en que se necesite.
- La institución deberá identificar mecanismos que permitan que las actividades de respaldo y recuperación de la información sean adecuadas costo / beneficio.
- Los niveles de protección y clasificación establecidos para la información de la institución deberán ser mantenidos en todo momento. (Acceso, toma de respaldo, backup, transporte, recuperación, otros). Por lo tanto, se deben mantener los controles y medidas establecidas para esto.
- Los usuarios de la entidad son responsables de la información institucional que manejan. Durante el mantenimiento preventivo se realiza una copia, la cual debe conservar y enviar una copia de respaldo al archivo institucional central.
- Los usuarios respaldan y protegen la información que manejan, con medidas que eviten accesos de personas no autorizadas. Se deberán preservar los lineamientos de acuerdo con la sensibilidad y nivel de clasificación de seguridad.
- El funcionario encargado de Sistemas o quien haga sus veces es la responsable del respaldo de las bases de datos a las que tenga acceso y deberá tener copia en varios espacios como garantía de continuidad de la institución.
- Los usuarios de la institución deberán seguir los procedimientos de respaldo de la información y crear inventario de copias de la información de los medios donde se haya guardado la información local y enviada al

archivo central, para facilitar el seguimiento de la actividad de seguridad y restauración.

- Quien haga las veces de control interno es la responsable del respaldo de las bases de datos a las que tenga acceso y deberá tener copia en varios espacios como garantía de continuidad de la institución.

7.3.3. Adquisición del software.

La centralización de las necesidades tecnológicas entre ellas la adquisición de software, permiten beneficiar la entidad en el control de costos por la puntualización de licencias correctas que causa descuentos, redistribución del software con otras dependencias, entre otras.

Los usuarios y funcionarios que requieran la adquisición de software deberán presentar el requerimiento a la Dirección operativa quien se encargará de evaluar el tipo de software, los requerimientos de instalación, el tipo de licencia, entre otras características que permita analizar la viabilidad de la adquisición. Por otra parte, si lo que requiere el usuario o empleado es la instalación de software específico individual que sea propiedad de la **Contraloría Municipal de Dosquebradas**, deberá solicitarlo por escrito a la Dirección operativa administrativa y financiera para que sea esta quien verifique la capacidad de la licencia o si debe adquirirse una adicional. Será una falta grave que los usuarios o funcionarios instalen cualquier tipo de software en sus computadoras conectado a la red de la **Contraloría Municipal de Dosquebradas** y que no esté autorizado previamente por el jefe inmediato y la Dirección operativa administrativa y financiera.

8. CONTROL DE ACCESO

Dentro del tipos de acceso están los accesos virtuales, que se relacionan con accesos lógicos a base de datos, aplicaciones en red, sistemas informáticos en general, entre otros.

8.1. Políticas de acceso a los sistemas de información.

8.1.1. Permisos.

Los sistemas de información de la **Contraloría Municipal de Dosquebradas** son fundamentalmente para uso exclusivo de las actividades institucionales. El uso personal de cualquier sistema de información para acceder, descargar, transmitir, distribuir o almacenar material o información distinta a la requerida para el normal desempeño de sus funciones está totalmente negado y sometido a sanciones disciplinarias y penales. Los recursos de sistemas de información o equipo sean usados con el objeto de obtener ganancia económica personal para cualquier usuario está igualmente negado por la entidad.

8.1.2 Acceso.

La **Contraloría Municipal de Dosquebradas** prohíbe el acceso no autorizado a los sistemas de información. Ningún usuario o funcionario debe usar la

identificación, identidad o contraseña de otro usuario, y de la misma manera No podrán dar a conocer su contraseña o identificación, excepto en casos que faciliten la reparación o el mantenimiento de algún servicio o equipo única y exclusivamente al personal de soporte de Sistemas o quien haga sus veces

8.1.3. Privacidad.

La **Contraloría Municipal de Dosquebradas** no garantiza la Privacidad de los Usuarios, aunque los sistemas de información de tipo laboral funcionen correctamente, porque estos pueden ser vulnerados por usuario que pueden revelarlo a otros. Los usuarios deben entender que ningún sistema de información es completamente seguro, que es muy posible que personas dentro y fuera de la institución puedan encontrar formas de tener acceso a la información. Por lo tanto, La Institución implementara todos los recursos, herramientas y acciones encaminadas a proveer un entorno de privacidad de los sistemas de información.

8.1.4. Seguridad en el correo electrónico.

El propósito de esta política es asegurar la privacidad de los mensajes de correo electrónico, el buen uso del sistema y el compromiso inherente de la institución al suministrar este servicio al personal. La información confidencial no debe ser transmitida por correo electrónico, a menos que una persona con autoridad directiva, de acuerdo con el cargo lo autorice.

- El personal de la **Contraloría Municipal de Dosquebradas** no puede emplear direcciones de correo electrónico diferentes a las cuentas oficiales para atender asuntos de la institución.
- Todos los mensajes de correo electrónico que utilizan los sistemas de información de la **Contraloría Municipal de Dosquebradas** deben contener el nombre y apellidos del remitente, su cargo, dirección y número telefónico.
- La solicitud de creación de cuenta de correo será realizada por la persona o dependencia previamente autorizada.
- Las cuentas de correo electrónico para personal de planta y contratistas serán creadas de forma personales (el nombre y primer apellido separado por un punto), esto permitirá ampliar la comunicación institucional además de poder hacer buen seguimiento de la gestión de correos.
- Un mensaje de correo electrónico debe ser retenido y conservado para futuras referencias solamente si contiene información relevante para la finalización de una transacción, si contiene información de referencia potencialmente importante o si tiene valor como evidencia de una decisión administrativa de la **Contraloría Municipal de Dosquebradas**.

La Contraloría Municipal de Dosquebradas debe comunicar a todos los usuarios que los sistemas de correo electrónico, que solamente deben ser utilizados para propósitos institucionales, todos los mensajes enviados por correo electrónico constituyen registros de la institución, quien se reserva el derecho de acceder y revelar cualquier mensaje para cualquier intento sin previo aviso y los administradores pueden revisar el correo electrónico del personal para determinar si han roto la seguridad, han violado la política de la

Contraloría Municipal de Dosquebradas o han realizado actividades no autorizadas.

- Los usuarios no pueden crear, enviar, o transmitir mensajes de correo electrónico que puedan constituir acoso o que puedan contribuir a un ambiente de trabajo hostil.
- Los usuarios de la **Contraloría Municipal de Dosquebradas** no pueden enviar o distribuir cualquier mensaje a través del correo electrónico de la institución, el cual pueda ser considerado difamatorio, acosador o de tipo de contenido sexual o que pueda ofender a alguien respecto a la raza, el género, la nacionalidad, orientación sexual, religión, política o discapacidad.
- El personal no debe utilizar los sistemas de la **Contraloría Municipal de Dosquebradas** para la transmisión de cualquier correo masivo no solicitado y que no sea persona autorizada para realizarlo.
- En todos los mensajes de correo electrónico salientes, debe agregarse un pie de página que indique que el mensaje puede contener información confidencial, que es para el uso de los destinatarios nombrados, que ha sido registrado para propósitos de archivo, que puede ser analizado por otras dependencias de la institución.
- El personal de la **Contraloría Municipal de Dosquebradas** no debe emplear versiones digitalizadas de la firma manuscritas en los mensajes de correo electrónico.
- Para contribuir con el medio ambiente, en todos los mensajes de correo electrónico deberá colocarse la reflexión respecto a no imprimir el correo electrónico si realmente no lo requiere para contribuir con la conservación.

8.1.5. Página Institucional.

El personal de la institución encargado de la información publicada en la Web será dirección operativa administrativa y financiera será quien garantice la disponibilidad del portal en producción en Internet.
Los estándares para la publicación de contenidos en la página web de la **Contraloría Municipal de Dosquebradas** estarán establecidos en la política de gobierno digital, la cual deberá ser seguida por el personal.

8.2 Controles de acceso lógico.

- El acceso a los sistemas de información de la **Contraloría Municipal de Dosquebradas** para personal externo debe ser autorizado por el Administrador del Sistemas de Información, quien deberá notificarlo por escrito a la dirección operativa administrativa y financiera.
- Está prohibido que los usuarios utilicen la infraestructura tecnológica de la institución para obtener acceso no autorizado a la información u otros sistemas de información gubernamentales.
- Todos los usuarios que utilicen unos servicios de información serán responsables por identificar el usuario y contraseña que recibe para el uso y acceso de los recursos.

- Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por cada sistema de información institucional, previa autorización por escrito por el administrador de este.
- Los usuarios no deben proporcionar información a personal externo, sobre los mecanismos de control de acceso a los sistemas de información institucionales.
- Está prohibido que los usuarios de la Institución compartan su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo verificación de que fueron usurpados esos (controles).

8.3 Administración de privilegios

- Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso al sistema de información al que pertenece como usuario de la **Contraloría Municipal de Dosquebradas**, deberá ser notificados por escrito o vía correo electrónico al administrador para la realización de los ajustes pertinentes.

8.4 Administración y uso de contraseñas

- La asignación de la contraseña para acceso a unos sistemas de información institucional debe ser realizada de forma individual, por lo que está prohibido el uso de contraseñas compartidas.
- Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por escrito al administrador de los sistemas de información al que por su labor debe gestionar, indicando los módulos al que accede, para que se le proporcione una nueva contraseña.
- Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera que se permita a personas no autorizadas su conocimiento. Los usuarios deberán tener en cuenta los siguientes lineamientos para la construcción de las contraseñas:

    - Deben estar compuestos por caracteres deben ser alfanuméricos, o sea, números y letras mayúsculas y minúsculas. Y caracteres especiales.
    - Que no sean fáciles de identificar, lo que quiere decir que no deben relacionarse con el nombre de usuario, el puesto de trabajo, la vida personal del usuario, entre otras que se descubra fácilmente.
    - Deben ser diferentes a las contraseñas que se hayan usado anteriormente.

- Todo usuario que tenga la sospecha que la contraseña ha podido ser identificada o conocida por otra persona, tendrá la obligación de cambiarlo inmediatamente.

8.5 Control de acceso remoto

- Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno de la dirección operativa a la que pertenezca.
- La administración remota de equipos conectados a internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por la dirección operativa a la que pertenezca.

9. PRIVACIDAD Y CONFIDENCIALIDAD

9.1 Privacidad y confidencialidad

Esta política contiene una descripción de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente.

9.1.1 Derechos de los titulares

Acorde con la Ley 1581 de 2012, en la **Contraloría Municipal de Dosquebradas**, reconoce los derechos de los titulares de los datos, así:

- ✓ Conocer, actualizar y rectificar sus datos personales.
- ✓ Solicitar la prueba de su autorización para el tratamiento de sus datos personales.
- ✓ Ser informado respecto del uso que se les da a sus datos personales.
- ✓ Revocar la autorización y/o solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo considere, siempre y cuando no se encuentren vigentes los servicios o productos que dieron origen a dicha autorización.
- ✓ Presentar quejas ante la entidad administrativa (Superintendencia de Industria y Comercio) encargada de la protección de los datos personales.

9.1.2 DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO (Ley 1581 de 2012)

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.
c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que

previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.
i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.
k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.
l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
m) Informar a solicitud del Titular sobre el uso dado a sus datos.
n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

9.1.3 DEBERES DE LOS ENCARGADOS DEL TRATAMIENTO (Ley 1581 de 2012)

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la Ley 1581 de 2012.
d) Actualizar la información reportada por los responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la Ley 1581 de 2012.
f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley 1581 de 2012 y, en especial, para la atención de consultas y reclamos por parte de los Titulares.
g) Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la Ley 1581 de 2012.
h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia Industria y Comercio.

9.2 Organización interna

- Los activos de información deben estar bajo la responsabilidad del responsable del activo, para evitar conflicto y reducir oportunidades de modificación (intencional o no), no autorizada o mal uso de los activos de información de la **Contraloría Municipal de Dosquebradas**.
- La dirección operativa administrativa y financiera debe mantener y documentar los contactos con autoridades (Policía, bomberos, etc.) u otros especializados, con el fin de contactar en caso de que se presente un incidente de seguridad de la información y requiera de asesoría externa.
- La **Contraloría Municipal de Dosquebradas** a través de la dirección operativa administrativa y financiera y demás personal que se determine, debe mantener contacto con grupos de interés especializados en seguridad y privacidad de la información, con el fin de compartir e intercambiar conocimientos, que permita la mejora continua del Sistema de Gestión de Seguridad de la Información de la entidad.
- Los proyectos que se desarrollen en la **Contraloría Municipal de Dosquebradas** deben contemplar una gestión de los riesgos de seguridad asociados a la información del proyecto, lo cual incluye una identificación de los riesgos y la definición de la forma como serán gestionados.
- En cualquier caso, los proyectos desarrollados por la **Contraloría Municipal de Dosquebradas** deben estar alineados a las políticas de seguridad contenidas en el presente manual.

9.3 Teletrabajo – trabajo en casa

- La dirección operativa administrativa y financiera debe establecer los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos, contratistas la **Contraloría Municipal de Dosquebradas**, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.
- Toda información gestionada la **Contraloría Municipal de Dosquebradas**, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales.

10. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

10.1 Identificacion De Procesos Y Servicios Principales Procesos de Software Identificados:

- Presupuesto
- Contabilidad
- Tesoreria

Principales servicios que deberán ser restablecidos y/o recuperados

Windows:

- Correo Electrónico.
- Internet.
- Antivirus.
- Herramientas de Microsoft Office.
- Software Base
- Backup de la Información.
- Ejecutables de las aplicaciones.
- Respaldo de la Información

10.2 Analisis De Evaluacion De Riesgos Y Estrategias

Metodología aplicada:

Para la clasificación de los activos de las Tecnologías de Información de la
Contraloría Municipal de Dosquebradas se han considerado tres criterios:

- **Grado de negatividad:** Un evento se define con grado de negatividad (Leve, moderada, grave y muy severo).
- **Frecuencia del Evento:** Puede ser (Nunca, aleatoria, Periódico y continuo)
- **Impacto:** El impacto de un evento puede ser (Leve, moderado, grave y muy severo).

Plan de Contingencia: Son procedimientos que definen como una entidad continuará o recuperará sus funciones críticas en caso de una interrupción no planeada. Los sistemas son vulnerables a diversas interrupciones, que se pueden clasificar en:

Leves: (Caídas de energía de corta duración, falla en la conexión a Internet)
Severas: (Destrucción de equipos, fallas en disco duro, incendios, entre otros.)
Riesgo: Es la vulnerabilidad de un Activo o bien, ante un posible o potencial perjuicio o daño.

Existen distintos tipos de riesgo:

- **Riesgos Naturales:** Tales como vendavales, lluvias torrenciales, tormentas eléctricas, terremotos.

- **Riesgos Tecnológicos:** Tales como incendios por causas eléctricas, fallas de energía y accidentes de transmisión y transporte.

- **Riesgos Sociales:** Como actos terroristas y desordenes callejeros.

Para realizar un análisis de todos los elementos de riesgos a los cuales está expuesto el conjunto de equipos informáticos y la información procesada de la entidad iniciaremos describiendo los activos que se pueden encontrar dentro de las tecnologías de información de la entidad:

Activos susceptibles de daño

- Hardware
- Equipos de protección como UPS
- Software y utilitarios
- Datos e información
- Documentación
- Suministro de energía eléctrica
- Suministro de telecomunicaciones e internet.

Posibles riesgos.

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, por causas naturales o humanas.

- Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

- Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia. Fuentes de daño

- Acceso no autorizado

- Ruptura de las claves de acceso a los sistemas computacionales.

- Desastres Naturales (Movimientos telúricos, Inundaciones, Fallas en los equipos de soporte causadas por el ambiente, la red de energía eléctrica o el no acondicionamiento atmosférico necesario.

- Fallas de Personal Clave (Enfermedad, Accidentes, Renuncias, Abandono de sus puestos de trabajo y Otros).

- Fallas de Hardware (Falla en los Servidores o Falla en el hardware de Red, Switches, cableado de la Red, Router, FireWall).

- Lentitud y caídas en el internet retrasando el trabajo.

Clases de Riesgos

- Incendio
- Robo común de equipos y archivos
- Falla en los equipos
- Equivocaciones
- Acción virus informático
- Fenómenos naturales

10.3 Minimizacion Del Riesgo

Teniendo en cuenta lo anterior, corresponde al presente Plan de Contingencia minimizar estos índices con medidas preventivas y correctivas sobre cada caso de Riesgo. Es de tener en cuenta que en lo que respecta a Fenómenos naturales, nuestra región ha registrado en estos últimos tiempos movimientos telúricos de poca intensidad; sin embargo, las lluvias fuertes producen mayores estragos, originando filtraciones de agua en los edificios de techos, produciendo cortes de energía, cortos circuitos (que podrían desencadenar en incendios).

INCENDIO
Grado de Negatividad: Muy Severo
Frecuencia de Evento: Aleatorio
Grado de Impacto: Alto

SITUACIÓN ACTUAL	ACCIÓN CORRECTIVA
La oficina donde están ubicados los equipos de cómputo cuenta con un extintor cargado, ubicado muy cerca a esta oficina y el Director de recurso humano.	Se cumple.
Fue capacitado el personal sobre el uso de elementos de seguridad y primeros auxilios, para enfrentar un incendio y sus efectos	Actividad realizada el 30 de noviembre de 2020.
El equipo de computo adscrito al Despacho del Contralor. Almacena información relacionada con la correspondencia recibida y entregada	Dado el gran volumen y la escaza capacidad que presenta el correo electronico se optó por almacenar la informacion en un disco duro externo igualmente se está almacenando informacion en DRIVE.

Dada la situacion vivida en el año 2020, COVID 19, donde se determinó el trabajo desde casa, como prevencion de salud pública, los archivos en su 80%, del proceso auditor se encuentran en forma digital	Adquiri espacio en la nube con dominio de la contraloría, destinar recurso para atender este estado de contingencia.

Analizando el riesgo de incendio, permite resaltar el tema sobre el lugar donde almacenar los Backup. El incendio, a través de su acción calorífica, es más que suficiente para destruir los Dispositivos de almacenamiento, tal como CD's, DVD's, Discos duros. Para la mejor protección de los dispositivos de almacenamiento, se colocarán estratégicamente en lugares seguros. Uno de los dispositivos más usados para contrarrestar la contingencia de incendio, son los extinguidores. Su uso conlleva a colocarlos cerca del las posibles áreas de riesgo que se debe proteger.

ROBO COMÚN DE EQUIPOS Y ARCHIVOS
Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio
Grado de Impacto: Alto

SITUACION ACTUAL	ACCION CORRECTIVA
No contamos con un sistema de seguridad, que controle la entrada y salida de personas ajenas a la Contraloría.	Se requiere que cada funcionario en el momento de retirarse de la oficina por un tiempo considerable, opte por guardar su equipo dentro de algún cajón bajo llave y la informacion contenida en el. Avisar a los compañeros para que estén pendientes de sus bienes mientras dure su ausencia.
Autorización escrita firmada por el Director Administrativo y Financiero de la Entidad para la salida de equipos de la Contraloría	Se cumple por medio del formato establecido para salida de equipos.

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos, sin el debido conocimiento y autorización del Director Operativo Administrativo y Financiero (E), esto demuestra que los equipos se encuentran bajo custodia y responsabilidad de cada funcionario autorizado.

Según antecedentes de otras entidades, es de conocer que en el robo de accesorios y equipos informáticos, llegaron a participar personal propio de la empresa en asocio con el personal de vigilancia, es relativamente fácil remover un disco duro del CPU, una disquetera, tarjeta, etc. y no darse cuenta del faltante hasta días después.

Estas situaciones no se han presentado en nuestro Ente de Control, pero se recomienda siempre estar alerta

FALLA EN LOS EQUIPOS
Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio
Grado de Impacto: Grave

SITUACION ACTUAL	ACCION CORRECTIVA
La falla en los equipos muchas veces se debe a falta de mantenimiento y limpieza.	Realizar mantenimiento preventivo de equipos por lo menos una vez al año.
La falla en el hardware de los equipos requiere de remplazo de repuestos de forma inmediata.	Contar con proveedores en caso de requerir remplazo de piezas y de ser posible contar con repuestos de quipos que están para dar de baja.
El daño de equipos por fallas en la energía eléctrica, requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Se cumple. En la Contraloría Municipal, en su mayoría cuenta con portátiles por tanto se recomienda que cada funcionario mantenga cargado su equipo y la UPS está funcionando.

Teniendo en cuenta la importancia del fluido eléctrico para el funcionamiento de la entidad, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongará por tiempo indefinido provocaría un trastorno en las operaciones del día, sin afectar los datos. Para el adecuado funcionamiento de las computadoras personales de escritorio, necesitan de una fuente de alimentación eléctrica fiable, es decir, dentro de los parámetros correspondientes. Si se interrumpe inesperadamente la alimentación eléctrica o varia en forma significativa (fuera de los valores normales), las consecuencias pueden ser muy serias, tal como daño del Hardware y la información podría perderse. La fuente de alimentación es un componente vital de los equipos de cómputo, y soportan la mayor parte de las anomalías del suministro eléctrico. Por lo anterior se debe tener en cuenta lo siguiente:

TOMAS A TIERRA O PUESTAS A TIERRA:

Se denomina así a la comunicación entre el circuito Eléctrico y el Suelo Natural para dar seguridad a las personas protegiéndolas de los peligros procedentes de una rotura del aislamiento eléctrico. Estas conexiones a tierra se hacen frecuentemente por medio de placas, varillas o tubos de cobre enterrados profundamente en tierra húmeda, con o sin agregados de ciertos componentes de carbón vegetal, sal o elementos químicos, según especificaciones técnicas indicadas para las instalaciones eléctricas. En la práctica protege de contactos accidentales las partes de una instalación no destinada a estar bajo tensión y

para disipar sobretensiones de origen atmosférico o industrial. La Toma a Tierra tiene las siguientes funciones principales:

a) Protege a las personas limitando la tensión que respecto a tierra puedan alcanzar las masas metálicas.

b) Protege a personas, equipos y materiales, asegurando la actuación de los dispositivos de protección como: pararrayos, descargadores eléctricos de líneas de energía o señal, así como interruptores diferenciales.

c) Facilita el paso a tierra de las corrientes de defecto y de las descargas de origen atmosférico u otro.

Fusibles

Si una parte de una computadora funde un fusible o hace saltar un diferencial, primero se debe desconectar el equipo, a continuación, debe desconectarse el cable de alimentación que lleva al equipo y buscar la falla que ha hecho saltar el fusible., una vez arreglado el problema se puede volver a conectar el equipo. Al sustituir un fusible, se ha de tener cuidado que todos los equipos deben estar apagados y desconectados antes de cambiar el mismo. No se debe olvidar que algunos elementos del equipo, como es el caso de los monitores, pueden mantener una carga de alto voltaje incluso, después de haberse apagado, asegurarse que el fusible de recambio es de la misma capacidad que el fundido. No aprobar las reparaciones de los fusibles, usando hilos de cobre o similares.

Extensiones eléctricas y capacidades

Las computadoras ocupan rápidamente toda la toma de corriente. Pocas oficinas se encuentran equipadas con las suficientes placas de pared. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser controlado con cuidado. No solo para que no queden a la vista, sino también porque suponen un peligro considerable para aquellos que tengan que pasar por encima. A parte del daño físico que puede provocar engancharse repentinamente con el cable, apaga de forma rápida un sistema completo.

EQUIVOCACIONES MANEJO DEL SISTEMA
Grado de Negatividad: Moderado
Frecuencia de Evento:
Periódico Grado de Impacto: Moderado

SITUACIÓN ACTUAL	ACCIÓN CORRECTIVA
Equivocaciones que se producen de forma involuntaria, con respecto al manejo de información, software y equipos.	Realizar instrucción inicial en el ambiente de trabajo presentando las políticas informáticas establecidas para manejo de sistemas

Algunas veces el usuario que tiene conocimiento en informática intenta navegar por sistemas que no están dentro de su función diaria.	El encargado de los sistemas debe asignar permisos y privilegios a cada usuario de acuerdo a sus funciones.
La entrega de inventario es realizada por la Dirección Operativa Administrativa y Financiera de la Entidad.	La Dirección Operativa Administrativa y Financiera de la Entidad debe entregar inventario en lo referente a equipos de cómputo, licencias, antivirus y solicitar la creación inmediata del usuario con sus claves.

ACCIÓN DE VIRUS INFORMÁTICO
Grado de Negatividad: Muy Severo
Frecuencia de Evento: Continuo
Grado de Impacto: Grave

SITUACION ACTUAL	ACCION CORRECTIVA
Únicamente la Dirección Operativa Administrativa y Financiera es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo a su necesidad y de los recursos existente en la entidad,	Se cumple
Por medio del correo electrónico se obtienen virus constantemente.	Crear conciencia en los funcionarios de forma que únicamente se reciba Información de importancia para la entidad.

Los Virus informáticos han evolucionado de tal manera que hoy en día todos conocemos la importancia de tener un programa Antivirus en el computador y aun más importante es su actualización. Si tenemos un antivirus instalado pero no lo hemos actualizado, seguramente será capaz de encontrar los virus que intenten entrar en nuestros sistemas pero no será capaz de hacer nada con ellos, dado que esta información está contenida en las definiciones de virus. La actualización del Patrón de Definiciones de virus es vital y debe de hacerse como mínimo una vez a la semana.

FENÓMENOS NATURALES
Grado de Negatividad: Grave
Frecuencia de Evento:Aleatorio
Grado de Impacto: Grave

SITUACION ACTUAL	ACCION CORRECTIVA

En la última década no se han registrado urgencias por fenómenos naturales como terremotos o inundaciones.	Aunque la probabilidad de ocurrencia es baja se requiere tener en cuenta medidas de prevención en todos los casos.
Aunque existen épocas de lluvia fuertes, las instalaciones de la **Contraloría Municipal de Dosquebradas** están debidamente protegidas.	Tomar medidas de prevención al respecto.
La UPS que sostiene la energía en un apagón.	La UPS está en buenas condiciones y funcionando.

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos necesarios en los puntos que se instalen los Computadores, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar mediante su caída y/o destrucción la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, dispositivos de almacenamiento, discos con información vital, todo ello como respaldo de aquellos que se encuentren aun en las instalaciones de la institución.

EVENTOS CONSIDERADOS PARA EL PLAN DE CONTINGENCIA

Cuando se efectúa un riesgo, este puede producir un Evento, por tanto, a continuación, se describen los eventos a considerar dentro del Plan de Contingencia.

RIESGO	EVENTO
• Fallas Tarjeta de Red. • Fallas IP asignado. • Fallas Punto de Swicht. • Fallas Punto Pacht • Panel. Swicht • Fallas Punto de Red.	No existe comunicación entre servidor y equipo.
• Falla del UPS (Falta de Suministro eléctrico). • Virus. • Sobrepasar el límite de almacenamiento del Disco.	Fallas en el equipo de cómputo.
• Incapacidad. • Accidente. • Renuncia Intempestiva.	Ausencia parcial o permanente del personal de tecnología de la Información.
• Corte General del Fluido eléctrico.	Interrupción del fluido eléctrico durante la ejecución de los procesos.

• Incendio. • Sabotaje. • Corto Circuito • Terremoto	Destrucción Del Espacio Donde Están Los Computadores.

No hay comunicación entre Servidor y el equipo en la **Contraloría Municipal de Dosquebradas**.

1. Requerimiento del usuario, que no cuenta con acceso a la red.
2. El Encargado de sistemas o quien haga sus veces procederá a identificar el problema o solicitar ayuda al departamento de sistemas de la alcaldía.
3. Si se constata problema con el Pacht Panel, realizar cambio del mismo.
4. Si no se resuelve el problema proceder a constatar si existe problema en la tarjeta de red, en caso de afirmativo realizar cambio o arreglo de la misma.
5. Si persiste el problema revisar los puntos de red, utilizando el diagrama lógico.
6. Testear el cable UTP. Si existe daño, realizar el cambio del cable.
7. Realizar mantenimiento del punto de red del usuario y del gabinete de comunicaciones
8. Recuperación del sistema de red para el usuario.

Recursos de Contingencia

- Componentes de Reemplazo
- Diagrama Lógico de la red

Error de Memoria RAM

En este caso se dan los siguientes síntomas:

- El Computador no responde correctamente, por lentitud de proceso.
- Ante procesos mayores se congela el proceso.
- Arroja errores con mapas de direcciones hexadecimale.

Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro del computador puede deberse a una de las siguientes causas:

- Caída del computador por falla de software de red.
- Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
- Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna falla en los sistemas computacionales de la Contraloría Municipal; se debe tener en cuenta:

- Verificar el suministro de energía eléctrica.

- Realizar backup de archivos contenidos en los computadores, a excepción de la carpeta raíz.
- Cargar un Portátil que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del computador.
- Al término de la operación de reparación se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente. Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

Recursos de Contingencia

- Componente de Remplazo (Memoria, Disco Duro, etc.).
- Backup diario de información de los computadores en memorias USB u otros medios disponibles.
- Obtener la relación de los Sistemas de Información con los que cuenta la Contraloría Municipal de Dosquebradas, detallando usuarios, en que equipos se encuentran instalados y su utilidad.
- Conocer la ubicación de los backup de información.
- Contar con el diagrama lógico de red actualizado.

Recursos de contingencia

Asegurar que el estado de las baterías del UPS, se encuentren siempre cargadas.

1. Realizar pruebas para identificar posible problema dentro de la entidad
2. Si se evidencia problema en el hardware, se procederá a cambiar el componente
3. Si se evidencia problema con el software, se debe reinstalar el sistema operativo del computador servidor
4. Si no se evidencia falla en los equipos de la entidad, se procederá a comunicarse con la Empresa prestadora del servicio, para asistencia técnica.
5. Es necesario registrar la avería para llevar un historial que servirá de guía para futuros daños.
6. Realizar pruebas de operatividad del servicio.
7. Servicio de internet activo y mejorarlo.

Recursos Contingencia.

- Hardware
- Router
- Software
- Herramientas de Internet.

Destruccion de los computdores de la Contraloria

1. Contar con el inventario total de sistemas actualizado.
2. Identificar recursos de hardware y software que se puedan rescatar.
3. Salvaguardar los backup de informaciones realizadas.

4. Identificar un nuevo espacio para restaurar los computadores averiados
5. Presupuestar la adquisición de software, hardware, materiales, personal y transporte.
6. Adquisición de recursos de software, hardware, materiales y contratación de personal.
7. Iniciar con la instalación y configuración de los nuevos computadores.
8. Restablecer los backup realizados a los sistemas.
9. Tenerlos asegurados contra todo riesgo.

10.4 Plan De Recuperacion Y Respaldo De La Informacion

El costo de la Recuperación en caso de desastres severos, como los de un terremoto que destruya completamente el interior de edificios e instalaciones, estará directamente relacionado con el valor de los equipos de cómputo que no fueron informados oportunamente y actualizados en la relación de equipos informáticos asegurados que obra en poder de la compañía de seguros.

El Costo de Recuperación en caso de desastres de proporciones menos severas, como los de un terremoto de grado inferior a 07 o un incendio controlable, estará dado por el valor no asegurado de equipos informáticos e información más el Costo de Oportunidad, que significa, el costo del menor tiempo de recuperación estratégica, si se cuenta con parte de los equipos e información recuperados. Este plan de restablecimiento estratégico del sistema de red, software y equipos informáticos será abordado en la parte de Actividades Posteriores al desastre.

El paso inicial en el desarrollo del plan contra desastres, es la identificación de las personas que serán las responsables de la ejecución del Plan de contingencia. Por tanto se definen los siguientes responsables:

- **Director Operativo Administrativo y Financiero:** Sera responsable de llevar a cabo las acciones correctivas definidas anteriormente a fin de minimizar los riesgos establecidos.
- **Director Operativo Técnico**: Verificara la labor realizada por el Director OperativoAdministrativo y Financiero.
- **Oficina de Control Interno:** Evaluara la ejecución de acciones correctivas a fin de minimizar los riesgos.

Un Plan de Recuperación de Desastres se clasifica en tres etapas:

Actividades Previas al Desastre.
Actividades Durante el Desastre.
Actividades Después del Desastre.

Actividades previas aldesastre

Se considera las actividades de actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Entidad. Se establece los procedimientos relativos

a. Sistemas e nformación

Obtención y almacenamiento de los Respaldos de Información (BACKUP).

La Entidad deberá tener un inventaroi de los Sistemas de Información con los que cuenta, tanto los de desarrollo propio, como los desarrollados por empresas externas.

b. Equipos de Cómputo

Se debe tener en cuenta el catastro de Hardware, impresoras, scanner, módems, fax y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional). Se debe emplear los siguientes criterios sobre identificación y protección de equipos:

- Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.

- Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación.
- Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la institución.

c. Obtención y almacenamiento de Copias de Seguridad (Backup)

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la institución

Actividades durante el Desastre

Presentada la contingencia o desastre se debe ejecutar las siguientes actividades planificadas previamente:

Plan de Emergencias

La presente etapa incluye las actividades a realizar durante el desastre o siniestros, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o madrugada. Este plan debe incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, descritas a continuación:

a. Buscar Ayuda de Otras Instituciones

Es de tener en cuenta que solo se debe realizar acciones de resguardo de equipos en los casos en que no se pone en riesgo la vida de personas. Normalmente durante la acción del siniestro es difícil que las personas puedan afrontar esta situación, debido a que no están preparadas o no cuentan con los elementos de seguridad, por lo que las actividades para esta etapa del proyecto de prevención de desastres deben estar dedicados a buscar ayuda inmediatamente para evitar que las acciones del siniestro causen más daños o destrucciones.

- Se debe tener en toda Oficina los números de teléfono y direcciones de organismos e instituciones de ayuda.

- Todo el personal debe conocer la localización de vías de Escape o Salida: Deben estar señalizadas las vías de escape o salida.

- Instruir al personal de la entidad respecto a evacuación ante sismos, a través de simulacros, esto se realiza acorde a los programas de seguridad organizadas por Defensa Civil a nivel local u otros entes.

- Ubicar y señalizar los elementos contra el siniestro: tales como extintores, zonas de seguridad (ubicadas normalmente en las columnas), donde el símbolo se muestra en color blanco con fondo verde.

- Secuencia de llamadas en caso de siniestro: tener a la mano elementos de iluminación, lista de teléfonos de instituciones como: Compañía de Bomberos, Hospitales, Centros de Salud, Ambulancias, Seguridad.

b. Formación de Equipos

Se debe establecer los equipos de trabajo, con funciones claramente definidas que deberán realizar en caso de desastre. En caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.), se debe formar 02 equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y el otro para salvamento de los equipos informáticos, teniendo en cuenta la clasificación de prioridades.

c. Entrenamiento

Se debe establecer un programa de prácticas periódicas con la participación de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo a los roles que se hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se pueden realizar recarga de extintores, charlas de los proveedores, etc. Es importante lograr que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir; y tomen con seriedad y responsabilidad estos entrenamientos; para estos efectos es conveniente que participen los Directivos y Ejecutivos, dando el ejemplo de la importancia que la Alta Dirección otorga a la Seguridad Institucional.

Actividades después del desastre

Estas actividades se deben realizar inmediatamente después de ocurrido el siniestro, son las siguientes:

a. Evaluación de daños

El objetivo es evaluar la magnitud del daño producido, es decir, que sistemas se están afectando, que equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo. En el caso de la **Contraloría Municipal de Dosquebradas** se debe atender los procesos de Contabilidad, Tesorería, Presupuesto y demás Sistemas de Información primordiales para el funcionamiento de la Entidad, por la importancia estratégica. La recuperación y puesta en marcha de los computadores que alojan dichos sistemas, es prioritario.

b. Priorizar Actividades

La evaluación de los daños reales nos dará una lista de las actividades que debemos realizar, preponderando las actividades estratégicas y urgentes de nuestra institución. Las actividades comprenden la recuperación y puesta en marcha de los equipos de cómputo ponderado y los Sistemas de Información, compra de accesorios dañados, etc.

c. Ejecución de actividades

La ejecución de actividades implica la colaboración de todos los funcionarios, creando Equipos de Trabajo, asignando actividades. Cada uno de estos equipos deberá contar con un líder que deberá reportar el avance de los trabajos de recuperación y en caso de producirse un problema, reportarlo de inmediato al Directivo, brindando posibles soluciones.

Los trabajos de recuperación se iniciarán con la restauración del servicio usando los recursos de la institución, teniendo en cuenta que en la evaluación de daños se contempló y gestionó la adquisición de accesorios dañados.

La segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución y el buen servicio de nuestro sistema e Imagen Institucional.

d. Evaluación de Resultados

Una vez concluidas las labores de Recuperación de los sistemas que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, con que eficacia se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades, como se comportaron los equipos de trabajo, etc. De la evaluación de resultados y del siniestro, deberían de obtenerse dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencias y Seguridad de Información, y otra una lista de recomendaciones para minimizar los riesgos y perdida que ocasionaron el siniestro.

e. Retroalimentación de Actividades

Con la evaluación de resultados, podemos mejorar las actividades que tuvieron algún tipo de dificultad y reforzar los elementos que funcionaron adecuadamente.

11. . REGISTRO Y AUDITORÍA

11.1 Consideraciones sobre auditorias

- La dirección operativa administrativa y financiera debe planificar periódicamente actividades que involucren auditorias de los sistemas críticos en producción.
- La dirección operativa administrativa y financiera debe documentar los resultados de las auditorias de los sistemas de Información de la Contraloría Municipal de Dosquebradas.

Elaboró:	Revisó:	Aprobó
Fernan Alberto Cañas Ingeniero de sistemas y computación Contratista	**María del Pilar Loaiza H** Directora Operativa Administrativa y Financiera	**Margarita María Gallego Gutiérrez** Contralora Municipal (e)