“POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-2020, Y EL TRATAMIENTO DADO AL MISMO, DEL CONCEJO MUNICIPAL DE BARRANCABERMEJA

LA MESA DIRECTIVA DEL HONORABLE CONCEJO MUNICIPAL DE BARRANCABERMEJA, en uso de sus atribuciones legales y conforme a la Ley 136/94, la ley 872 de 2003 y el reglamento interno del Concejo Municipal y,

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

- Que el artículo 15 de la constitución política consagra el derecho de todas las personas a su intimidad personal y familiar y a su buen nombre, correspondiéndole al Estado su protección.

- Que el D 1078 de 2015, modificado por el D. 1008 de 2018, por el cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, en sus artículos 2.2.9.1.1.1 y 2.2.9.1.1.3 establece que la Política de Gobierno Digital se desarrollará a través de sus componentes y habilitadores transversales, es decir los elementos fundamentales de Seguridad de la Información e incluye a esta última entre los principios de la política de Gobierno Digital

- Que de conformidad con el artículo 2.2.9.1.1.2 ibídem, son sujetos obligados de las disposiciones contenidas en la norma en cita, todas las entidades que conforman la administración pública en los términos del artículo 39 de la ley 489 de 1998, así como los particulares que ejercen funciones administrativas.

- Que la adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización, sea pública o privada.

- Que la ley 1581 de 2012 por la cual se dictan disposiciones para la protección de datos personales, desarrolla el derecho constitucional de todas las personas a conocer, actualizar y rectificar la información que se recoja en bases de datos o archivos.

- Que la ley 1712 de 2014 por la cual se crea la ley de Transparencia y del derecho de Acceso a la Información Pública tiene como objetivo regular los procedimientos y garantías para el ejercicio de ese derecho.

- Que la ley 1955 de 2019 por la cual se expide el Plan Nacional de desarrollo 2018-2022 prevé el Pacto por la transformación digital de Colombia, con el que se persigue el uso y aprovechamiento de las TIC para mejorar la provisión de los servicios digitales, generando confianza y eficiencia en la toma de decisiones basadas en datos confiables y actualizados.

- Que la aplicación de este pacto por el buen uso de las Tecnologías de la Información y la Comunicación permitirá a las entidades públicas mejorar su funcionamiento y relación con otras entidades y con la ciudadanía.

- Que, por lo anterior, se hace necesario adoptar una Política General de Seguridad y Privacidad de la Información, implementando un Plan de Seguridad y privacidad de la Información en el Concejo Municipal de Barrancabermeja que permita cumplir los objetivos del pacto por la transformación digital.

- Que, en mérito de lo expuesto,

R E S U E L V E:

ARTÍCULO 1o. Adoptar el **PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2020** para el Concejo Municipal de Barrancabermeja, el cual se encuentra desarrollado en el anexo No 1 que forma parte integral de la presente resolución.

ARTÍCULO 2o. Adoptar el **PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2020** para el Concejo Municipal de Barrancabermeja, el cual se encuentra desarrollado en el anexo No 2 que forma parte integral de la presente resolución.

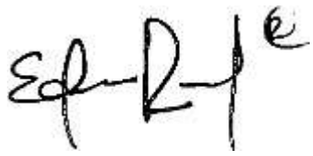
ARTÍCULO 3o. Los Planes aquí adoptados serán revisados al menos una vez al año y podrán ser actualizados de acuerdo con las normas que regulan la materia.

ARTICULO 4o. Vigencia. Los Planes aquí adoptados quedarán vigentes a partir de la fecha de expedición de la presente resolución y su aplicación será de obligatorio cumplimiento.

COMUNÍQUESE Y CUMPLASE

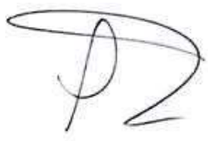
Expedida en Barrancabermeja a los nueve (09) días del mes de noviembre de dos mil veinte (2020).

DARINEL VILLAMIZAR RUIZ
Presidente

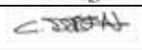


EDSON LEONIDAS RUEDA RUEDA
Primer Vicepresidente

JULIETT MARCELA RODRIGUEZ RINCON
Segundo Vicepresidente



RODOLFO RIOS BELTRAN
Secretario General

	NOMBRE	CARGO	FIRMA
Elaboró	Maritza Castellanos Guzmán	Abogada Externa	
Revisó	César Dorzan	Abogado externo	

GESTIÓN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2020

CONCEJO DISTRITAL
BARRANCABERMEJA

CONCEJO DISTRITAL DE BARRANCABERMEJA
SANTANDER – COLOMBIA - 2020

1. INTRODUCCION

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, está diseñado bajo la orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la corporación en caso de materialización, así mismo se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en la Gestión TIC para el desarrollo de los procesos misionales.

En el presente documento se establecerán las políticas de seguridad de la información que se deben cumplir para darle un manejo adecuado a su seguridad, permitiendo así su correcto tratamiento y respaldo.

1.2 OBJETIVO

Evitar el acceso no autorizado a las instalaciones al Concejo Distrital de Barrancabermeja, al centro de cómputo y a la información de la Corporación.

1.3 OBJETIVOS ESPECÍFICO

- Definir los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información que pueda estar expuesta, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.
- Gestionar los riesgos de Seguridad y Privacidad de la información, de acuerdo con los contextos establecidos en la corporación.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información.

1.4 GLOSARIO

- **Seguridad informática**: Se ocupa de la implementación técnica y de la operación para la protección de la información.
- **Seguridad de la información**: Se Ocupa de evaluar el riesgo y las amenazas, traza el plan de acción y esquemas normativos. Es la línea estratégica de las Seguridad.
- **Amenazas**: Cualquier evento, persona, situación o fenómeno que pueda causar daño.
- **Vulnerabilidades**: Falla o debilidad en un sistema que puede ser explotada por quien la conozca.

- **Riesgo**: Probabilidad de ocurrencia de una amenaza.
- **Controles**: Conjunto de mecanismos que regulan el funcionamiento de un sistema.
- **ISO**: Organización Internacional de Normalización es una organización para la creación de estándares internacionales.
- **Activo**: Bienes, recursos o derechos que tenga valor para una organización.
- **Activo de Información**: Toda la información que maneja con la que cuenta una organización para un correcto funcionamiento.
- **Análisis de brechas**: es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado.
- **Análisis de Riesgo**: Método empleado para evaluar los riesgos informáticos y obtener respuesta de peligro.
- **Gestión del Riesgo Informáticos**: Actividades empleadas para mitigar los riesgos informáticos.
- **Incidente de seguridad informática**: daño que puede comprometer las operaciones de la alcaldía municipal.
- **Evento**: Acción que puedo haber causado daño, pero fue controlado.
-
- **Información**: Conjunto de datos que tienen un significado.
-
- **Probabilidad**: Posibilidad de que una amenaza se materialice
- **Impacto**: Daño que provoca la materialización de una amenaza.
- **SGSI**: Sistema de Gestión de seguridad de la Información
- **MSPI**: Modelo de seguridad y privacidad de la información

2. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La información es uno de los activos más importantes de una organización por lo que su integridad, confidencialidad y disponibilidad debe, de cierta manera, estar bajo un nivel de adecuado de seguridad aceptable, cumpliendo con códigos de buenas prácticas de seguridad de la información.

En el presente documento se establecerán las políticas de seguridad de la información que se deben cumplir para darle un manejo adecuado a su seguridad, permitiendo así su correcto tratamiento y respaldo.

2.1 POLITICAS DE SEGURIDAD

El Plan de Seguridad y Tratamiento de la Información, contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos de información, estas actividades se estructuraron de la siguiente manera

RECURSO	OBJETIVO	RESPONSABLE	POLITICAS - PROCEDIMIENTOS
SEGURIDAD FÍSICA	**Diseñar y aplicar Políticas para el control de los accesos a las áreas físicas determinadas como de alto riesgo para filtración de información de la corporación.**	**Ingeniero Sistema**	**Áreas Restringidas a personal autorizado**: Evitar el acceso físico no autorizado a las instalaciones del Centro de Cómputo y Datos del Concejo Distrital de Barrancabermeja y a la información de la Corporación. **De los equipos servidores y de procesamiento**: Todos los servidores y los sistemas de procesamiento de información del Concejo Distrital de Barrancabermeja, deberá contar con perímetros de seguridad física adecuados que impidan el acceso no autorizado al mismo. **De los equipos activos de red**: Los dispositivos de red tales como routers, switches, se consideraran como área segura y deberá contener algún tipo de seguridad. Los empleados contratistas o terceros deberán abstenerse de moverlo, reubicarlo o de conectarse directamente a él sin la autorización previa del profesional responsable. **De los equipos de Cómputo**: Cada equipo de cómputo incluyendo periféricos como scanner, impresoras y fotocopiadoras, deberán tener un responsable designado, al cual se le hará entrega formal del equipo por medio de un acta firmada por cada una de las partes, este documento deberá contener las características y el estado inicial del activo. **Salida e Ingreso de Equipos externos:** Los equipos de cómputo o cualquier otro activo de información de propiedad del Concejo Distrital podrán salir de las instalaciones previa autorización del Secretario General o la persona responsable de la gestión de activos. Así mismo cualquier tercero que acceda a las instalaciones del Concejo Distrital de Barrancabermeja deberá registrar al momento de su ingreso: equipos de cómputo, equipos de comunicaciones.

EQUIPOS ACTIVOS DE COMUNICACIÓN	Diseño de políticas y procedimientos para el manejo adecuado de los dispositivos activos de red, tanto en protección física, como en su configuración lógica.	**Ingeniero Sistema**	**De los equipos activos de red:** Todos los equipos activos y de comunicación deberán estar correctamente identificados, por medio de un sticker, dicha identificación deberá ser única independientemente del tipo de activo que se esté etiquetando y tener una hoja de datos con la información de configuración y mantenimientos.
ACTIVOS DE INFORMACION	**Diseño de políticas para el control y seguimiento de los diferentes activos de información, de los Sistemas de Información, delos dispositivos de almacenamiento y respaldo**	**Ingeniero Sistema**	**De los sistemas de información:** Todos los sistemas de información del Concejo Distrital deberán tener su respectivo manual de usuario. **Acceso a los Sistemas de Información**: El acceso a los sistemas de información críticos como el Software financiero, deberá ser accedido únicamente desde equipos seguros, evitando el acceso desde equipos públicos o salas de internet. **De las copias de Seguridad:** Cada usuario es responsable de la información producida y derivada de su trabajo y de sus funciones. El usuario deberá realizar una copia de seguridad periódicamente de la información que consideren relevante.,
REDES Y TELECOMUNICACIONES	Diseño de políticas para Asegurar el correcto uso de la red de datos y de los servicios que se utilizan por ese medio.	**Ingeniero Sistema**	**Uso del correo electrónico Institucional:** El correo electrónico institucional es personal e intransferible, cada usuario mantiene su propia cuenta y está prohibido el utilizar cuentas asignadas a otras personas para enviar o recibir mensajes de correo, a menos que sea autorizado por el secretario del Concejo. **Acceso a redes públicas (Internet):** El acceso a Internet provisto para el personal del Concejo Distrital a través de la red es de uso exclusivo para el desarrollo de las actividades relacionadas con las necesidades del puesto y función que desempeña.

2.2 COMUNICACIÓN Y OPERACIÓN

RECURSO	OBJETIVO	RESPONSABLE	POLITICAS - PROCEDIMIENTOS
GESTION DE ACTIVOS	**Diseño de políticas y procedimientos para el manejo adecuado de la información.**	**Ingeniero Sistema**	• Todos los activos de información deberían estar correctamente identificación deberá ser única independientemente del tipo de activo que se esté etiquetando. • Siempre que se dé de baja un medio de almacenamiento como discos duros, memorias USB, entre otros, se debe destruir totalmente haciéndolos irrecuperables, así mismo debe quedar constancia de ello. • El procedimiento que se utilice para la eliminación del medio, deberá ser aquel que minimice el riesgo de fuga de la información.
PROTECCION DE LOS EQUIPOS DE COMPUTO	Diseño de políticas y procedimientos para el manejo adecuado de los dispositivos activos como los periféricos, tanto en protección física, como en su configuración lógica.	**Ingeniero Sistema**	• Cada equipo de cómputo incluyendo periféricos como scanner, impresoras y fotocopiadoras, deberán tener un responsable designado, al cual se le hará entrega formal del equipo por medio de un acta firmada por cada una de las partes, este documento deberá contener las características y el estado inicial del activo. • La ubicación de los equipos de escritorio y periféricos como impresoras, fotocopiadoras y scanner deberá ser la que menor riesgo tenga con respecto a posibles amenazas ambientales o accesos no autorizados, así mismo, el empleado o contratista deberá respetar dicha ubicación
SALIDA E INGRESO DE EQUIPOS	**Diseño de políticas para el control y seguimiento de los diferentes activos que entra o sale de la Corporación**	**Ingeniero Sistema**	• Cualquier tercero que acceda a las instalaciones de la Corporación de Barrancabermeja deberá registrar al momento de su ingreso: equipos de cómputo, equipos de comunicaciones (excepto por teléfonos móviles o celulares) y herramientas que no sean propiedad de la Corporacion, de manera que se mantenga control sobre el tráfico de los equipos de cómputo que entran y salen.

			• Los equipos de cómputo y de comunicaciones o cualquier otro activo de información de propiedad de la Corporación podrán salir de las instalaciones previa autorización de la persona responsable de la gestión de activos.
GESTIÓN DE ACTIVOS	**Diseño de políticas para Asegurar el correcto uso de los periféricos y de los servicios que se utilizan por ese medio.**	**Ingeniero Sistema**	• Todos los activos de información deberán estar correctamente identificados, por medio de una lámina o sticker, dicha identificación deberá ser única independientemente del tipo de activo que se esté etiquetando. • Siempre que se dé de baja un medio de almacenamiento como discos duros, memorias USB, entre otros, se debe destruir totalmente haciéndolos irrecuperables, así mismo debe quedar constancia de ello. • El procedimiento que se utilice para la eliminación del medio, deberá ser aquel que minimice el riesgo de fuga de información.
USO DE SOFTWARE	**Diseño de políticas de manejo de los procedimientos tecnológicos y de los servicios de procesamiento de información.**	**Ingeniero Sistema**	• Cualquier instalación de software deberá ser realizado o, autorizado y aprobado por el profesional responsable de sistemas. • Si se requiere el uso de software propietario, se deberá justificar el uso del mismo y solicitar la autorización al profesional responsable de sistemas indicando en que equipo o equipos deberá instalarse el programa. • El nivel de acceso que deberán tener los usuarios a sus equipos asignados, serán los mínimos que le permitan ejecutar de manera correcta y suficiente sus actividades diarias. En caso de que un usuario necesite privilegios de administrador en su sesión, ésta deberá ser aprobada y avalada por el profesional responsable de sistemas.

MANTENIMIENTO Y USO DE LOS EQUIPOS	**Diseño de políticas de manejo de los procedimientos tecnológicos y de los servicios de procesamiento de información.**	**Ingeniero Sistema**	• Solo el personal autorizado por el profesional responsable en sistemas realizará los mantenimientos y diagnósticos preventivos de los equipos de cómputo de la Personería Municipal de Barrancabermeja. • Las configuraciones de los equipos de cómputo solo pueden ser modificadas por el profesional responsable en sistemas. • Todo archivo o información descargada desde la red o desde medios removibles como memorias USB, discos duros portátiles, discos compactos, entre otros, deberá ser revisado por el software antivirus antes de su utilización o apertura.
Administración de Contraseñas.	**Diseño de políticas de seguridad para el manejo de las contraseñas que maneja la Corporación**	**Ingeniero Sistema**	• Los usuarios son responsables de la seguridad de sus contraseñas, tanto de su equipo como de los aplicativos a los cuales tiene acceso. Por ende, el usuario es responsable de todas las actividades realizadas con su nombre de usuario. • Los usuarios deberán cambiar su contraseña periódicamente y estas no deberán contener información personal como nombres o números de teléfono, con el fin de que no se pueda inferir la contraseña con dicha información. • Se debe evitar el almacenamiento de las contraseñas en papel o en registros digitales, a menos que estos tengan algún tipo de seguridad perimetral o de acceso. • Cuando un usuario olvide, bloquee o extravíe su contraseña deberá solicitar al profesional responsable en sistemas que le realice la acción que le permita ingresar una nueva contraseña, y al momento de recibirla deberá cambiarla por una nueva.

ACCESO A LOS SISTEMAS DE INFORMACION	**Diseño de políticas de seguridad para el manejo de las contraseñas que maneja la Corporación**	**Ingeniero Sistema**	• El acceso a los sistemas de información críticos como el Software financiero, deberá ser accedido únicamente desde equipos seguros, evitando el acceso desde equipos públicos o salas de internet. • Deberá evitarse el uso de la característica de los exploradores de "recordar usuario y contraseña", para evitar que personas no autorizadas accedan a los sistemas de información valiéndose de esto. • Los accesos a sistemas de información WEB o aplicaciones WEB, deberán accederse digitando directamente la dirección en la barra de direcciones del explorador o siguiendo los enlaces del portal WEB de la Corporación. En todo caso deberá evitar el uso de buscadores, marcadores o accesos directos. • Los privilegios establecidos a los usuarios en los sistemas de información deberán ser aprobados por el Secretario General.

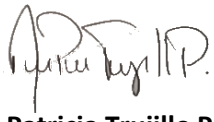
2.3 CUMPLIMIENTO

Asegurar el cumplimiento de normativas legales internas del Concejo Distrital de Barrancabermeja, así como cualquier ley que aplique en las respectivas labores.

2.3.1 Propiedad Intelectual.

Está prohibido por las normas de derechos de autor y por el Concejo Distrital de Barrancabermeja, realizar copias no autorizadas de software.

Los sistemas desarrollados por personal interno o contratistas son propiedad intelectual del Concejo Distrital de Barrancabermeja.



Proyecto: **Ana Patricia Trujillo Pazos**
Ingeniera de Sistemas

GESTIÓN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2020

CONCEJO DISTRITAL
BARRANCABEMERJA

CONCEJO DISTRITAL DE BARRANCABERMEJA
SANTANDER – COLOMBIA - 2020

1. INTRODUCCION

Si en un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, las consecuencias derivadas de sucesos posteriores y relevantes como el terrorismo, la inestabilidad política, las pandemias y los códigos maliciosos, entre otros, han señalado la necesidad de incorporar nuevas amenazas presentes no solamente en el mundo físico sino también en el entorno digital, cuando se trate de comprender los riesgos más significativos a los activos de información. El análisis de riesgos de los activos de información nos permite entender de una manera efectiva y eficiente los riesgos de pérdida de confidencialidad, integridad y disponibilidad sobre cada uno de los activos definidos como parte del alcance del análisis.

Gestionar eficazmente la seguridad de la información y riesgos de seguridad digital de los sistemas de información de la Corporación, así como en los activos que participan en sus procesos y que se encuentran expuestos, permite garantizar la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de las opciones apropiadas de tratamiento de riesgos de Seguridad de la información y seguridad digital, teniendo en cuenta la evaluación de los resultados de la valoración de los riesgos del Sistema de Gestión de Seguridad de la Información y en concordancia a la normativa aplicable.

Así mismo, este plan apoya la implementación de controles y acciones tendientes a la mitigación de los riesgos del proceso de gestión tecnológica, hallazgos de auditorías internas.

1.2 OBJETIVO

Proporcionar las directrices que permitan actuar adecuadamente frente a los riesgos que se enfrenta la gestión de las TIC, empleadas por la Corporación Distrital de Barrancabermeja.

1.3 OBJETIVOS ESPECIFICOS

- Identificar los riesgos asociados a los procesos y los activos de información que hacen parte del alcance del SGSI.
- Establecer el plan de tratamiento de riesgos.
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos.

1.4 DEFINICIONES

- **TIC:** Termino utilizado para las Tecnologías de la Información y Comunicación y son todas las tecnologías que permiten acceder, producir, guardar, presentar y transferir información. Gracias a estas, los campos de la educación, cultura, política, opinión y demás han logrado avanzar en la distribución y masificación de sus contenidos, planes de acción y trabajo y las diversas funcionalidades en sus áreas.

- **Seguridad informática**: Campo de la informática encargado de la protección y vigilancia de la infraestructura computacional, la cual comprende software, bases de datos, metadatos, archivos y todos aquellos elementos que la organización considere pueden estar en riesgo, como por ejemplo la información confidencial. En esa medida, a través de un sistema de mantenimiento y seguridad se establecen una serie de protocolos y medidas que pretenden evitar cualquier tipo de amenazas las cuales pueden ser causadas por usuarios o programas maliciosos. (CCD, 2012).

- **Informática:** Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras. (RAE, 2014).

- **Contingencia:** Suspensión, interrupción, inesperada y no planificada de la disponibilidad de los recursos tecnológicos, en otras es “la posibilidad de que algo suceda o no suceda” (RAE, 2014).

- **Copia de Seguridad (Backup):** Es el proceso de copia de seguridad con la finalidad de utilizarla para restaurar lo original después de una incidencia. De acuerdo a (ALESGA, 1998) es la copia total o parcial de información importante como respaldo frente a eventualidades. La copia de seguridad debería ser guardada en un soporte

almacenamiento diferente del original, para evitar que un fallo en el mismo pueda estropear el original y la copia.

- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

- **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.

- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

1.5 MARCO NORMATIVO

Decreto 1078 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1008 de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

CONPES 3854 de 2016 Política Nacional de Seguridad Digital.

Manual para la Implementación de la Política de Gobierno Digital Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019.

Modelo de Seguridad y privacidad de la información - MSPI Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales.

NTC / ISO 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

NTC/ISO 31000:2009 Gestión del Riesgo. Principios y directrices.

Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4 Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

2. MEDIDAS DE CONTIGENCIA

Se listan los riegos y acciones a ejecutar manifestada por la Corporación:

RIESGO: INCENDIOS Y EXPLOSIONES

ACCIONES A EJECUTAR:

Implementar las medidas de atención de contraincendios:

- Cerrar el circuito eléctrico de la zona afectada.
- Solicitar el apoyo al personal entrenado en uso de extintores para extinguir el fuego.
- Simultáneamente llamar e informar a los bomberos, para que brinde apoyo.
- Evaluar los daños y establecer las medidas de recuperación y restablecimiento el servicio.
- Apoyo de los sistemas automáticos de respaldo del sistema informático y recuperación de copias de respaldo programadas.
- Informar a la aseguradora.
- Adecuar la zona afectada e instalar los nuevos equipos, junto red de cableado estructurado. (cuando sea posible).
- Reubicar el puesto de trabajo y/o área afectada, e instalarla en un lugar provisional, mientras es restablecida la infraestructura.

RIESGO: CORTE DE ENERGÍA

ACCIONES A EJECUTAR:

- Entra en funcionamiento el sistema de alimentación de energía UPS mientras se hacen respaldos de las últimas actividades sobre los sistemas informáticos.

- Informar a la empresa proveedora de energía eléctrica y/o informar al administrador del edificio.

- En caso de que el corte de energía dure mayor de 2 días se procederá a solicitar un servicio de apoyo, mientras se supera la contingencia.

RIESGO: FALLAS EN HARDWARE O SOFTWARE

ACCIONES A EJECUTAR:

- Evaluar el origen de la falla para determinar las responsabilidades y proceder aplicar los correctivos.

- Apoyo de los sistemas automáticos de respaldo del sistema informático y recuperación de copias de respaldo programadas.

RIESGO: SABOTAJE O DAÑO ACCIDENTAL

ACCIONES A EJECUTAR:

- Apoyo de los sistemas automáticos de respaldo del sistema informático y recuperación de copias de respaldo programadas.

- Evaluar el sabotaje o daño accidental para determinar las responsabilidades y proceder aplicar los correctivos.

RIESGO: VANDALISMO Y MANIFESTACIONES

ACCIONES A EJECUTAR:

- Cierre de instalaciones temporal mientras se informa a las autoridades de fuerza pública.

- Apoyo de los sistemas automáticos de respaldo del sistema informático y recuperación de copias de respaldo programadas.

RIESGO: PANDEMIA

ACCIONES A REALIZAR:

- Tener un Servidor donde se encuentren todos los documentos que se maneja en la Corporación para que se acceda a ella desde cualquier lugar.

- Evaluar la posibilidad de una Intranet donde se encuentre centralizada todos los documentos que se maneja en la corporación.

- Importancia tener todos los documentos en medios digitales para trabajarlo desde una herramientas digital.

2.1 ELEMENTOS SUSCEPTIBLES DE CONTINGENCIA

Se identificaron algunos elementos que pueden ser perturbados y susceptibles de la contingencia: -

- ✓ Equipos de cómputo.
- ✓ Impresoras.
- ✓ Sistemas de Información.

2.2. REVISIÓN Y ACTUALIZACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La revisión y actualización se realizará en el tiempo de cada vigencia, allí se actualizarán las medidas de contingencia frente a nuevos hallazgos que sean identificados.

Proyecto: **Ana Patricia Trujillo Pazos**
Ingeniera de Sistemas