ANEXO 9.

MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONCEJO DISTRITAL DE CARTAGENA DE INDIAS

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Para la entidad Concejo Distrital de Cartagena de Indias es de gran importancia contar con un marco que asegure la información de la entidad dentro delos criterios de disponibilidad, confiabilidad e integridad todo esto dentro de un sistema de gestión de seguridad de la información (SGSI), de ahí la necesidad de contar con políticas claras para la protección de la información que produce la entidad.

La razón de este manual es describir las políticas de seguridad de la información definidas por la Concejo Distrital de Cartagena de Indias. Para la elaboración del mismo, se toma como base el Anexo A, incluido en la norma ISO 27001:2013, recomendaciones de la ISO 27002:2013 los lineamientos de la estrategia de Gobierno en Línea (GEL), en especial las guías suministradas.

Las políticas de seguridad de la información incluidas en este manual constituyen una parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno en Línea (GEL) y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La preservación de la confidencialidad, integridad y disponibilidad de la información para la Concejo Distrital de Cartagena de Indias, constituye una prioridad y por tanto, es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

2. OBJETIVO

Contar con políticas de seguridad de la información que le permitan al Concejo Distrital de Cartagena cumplir con los estándares de seguridad de la información que establece la norma.

3. ALCANCÉ

En el presente manual se establecen las políticas de seguridad de la información de las áreas de atención al usuario, dirección administrativa y dirección financiera del Concejo Distrital de Cartagena de Indias en miras a cumplir con los objetivos institucionales. Las políticas de seguridad de la información establecidas en el presente documento cumplen un papel primordial para el desarrollo de los procesos de las áreas por lo cual deberán ser conocidas y cumplidas por todos los servidores públicos, contratistas proveedores y partes interesadas, que accedan a los sistemas de información y a la infraestructura física de la entidad.

4. TIEMPO DE VALIDEZ

Cada año se revisarán las políticas contenidas en este manual con el fin de verificar su funcionamiento y si es necesario realizar algún tipo de cambio que permita el mejoramiento de las políticas de seguridad de la información y por ende el mejoramiento del sistema

5. TÉRMINOS Y DEFINICIONES

- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000)
- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000**).**
- **Confidencialidad:** Protege a la información de que esté disponible a usuarios, entidades o procesos no autorizados.
- **Análisis de riesgos de seguridad de la información:** proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.
- **Autenticidad:** Permite que la información transmitida o intercambiada provenga de fuentes auténticas y de quiénes dicen ser que son**.**
- **Autenticación:** es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
- **Centros de cableado:** Es el lugar donde se instalan los cables y dispositivos de comunicación. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.
- **Cifrado:** es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El

cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

- **Confidencialidad:** es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **Criptografía:** es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.
- **Custodio**: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado (ISO/IEC 27002:2013)
- **Derechos de Autor:** es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.
- **Disponibilidad**: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. (ISO/IEC 27002:2013)
- **Equipo de cómputo:** dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
- **Incidente de Seguridad**: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

- **Integridad:** Permite que la información sea correcta y que no haya sido alterada por usuarios, entidades o procesos no autorizados**.** Propiedad de salvaguardar la exactitud y estado completo de los activos (ISO/IEC 27002:2013)
- **Licencia de software:** es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.
- **Medios removibles:** Todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores.
- **Perfiles de usuario:** son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.
- **Propiedad intelectual:** es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.
- **Propietario de la información:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso (ISO/IEC 27002:2013)

- **Recursos tecnológicos:** son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad,

servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior del Concejo Distrital De Cartagena de Indias.

- **Registros de Auditoría:** son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos del instituto. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.
- **Responsable por el activo de información:** es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Sistema de información:** es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por el Concejo Distrital de Cartagena de Indias o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.
- **Software malicioso:** es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.
- **Terceros:** todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.
- **Vulnerabilidades:** son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores

externos y no controlables por el instituto (amenazas), las cuales se constituyen en fuentes de riesgo.

6. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Con el objetivo de lograr el cumplimiento de las políticas de seguridad de la información y generar una cultura de seguridad en la entidad, las violaciones a las políticas constituirán medidas disciplinarias o penales si lo ameritan

7. LINEAMIENTOS GENERALES

- Cualquier tipo de contratación o convenio que celebre la entidad debe contener una clausula donde el contratista acepte el cumplimiento de las políticas de seguridad de la información, por lo cual se firmara un acta de compromiso de confidencialidad de la información.
- Todas las actualizaciones que se realicen al manual de seguridad de la información serán de conocimiento a los funcionarios, servidores públicos, contratistas, estas serán comunicadas a través de los medios establecidos para este fin.
- Las acciones realizadas en los equipos tecnológicos y en las aplicaciones informáticas a través de usuario y contraseña quedan registradas y las consecuencias legales acerca de malos procedimientos serán asumidos por los usuarios.

8. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CONCEJO DISTRITAL DE CARTAGENA

El Concejo Distrital de Cartagena, teniendo claridad de la importancia de una adecuada Gestión de la información, se compromete con el diseño y puesta en marcha de un Sistema de gestión de seguridad de la información con el fin de establecer un marco de confianza en el ejercicio de sus deberes con el estado y los ciudadanos, enmarcándose en el cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para el Concejo Distrital de Cartagena, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

La política general de seguridad y privacidad de la información del Concejo Distrital de Cartagena sea aplicara a la entidad de acuerdo al alcance, los funcionarios, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.

- 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, y clientes del Concejo Distrital de Cartagena.
- Garantizar la continuidad del negocio frente a incidentes.

EL CONCEJO DISTRITAL DE CARTAGENA ha decidido definir 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.

9. POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

9.1. Política de estructura organizacional de seguridad de la información.

Objetivo:

El Concejo Distrital de Cartagena de Indias establece y garantiza la conformación de un Comité de Seguridad de la Información, definiendo roles y responsabilidades, esto permitirá gestionar en forma oportuna los incidentes de violación de seguridad detectados.

Alcance:

Comprende todo el personal desde la alta dirección hasta los colaboradores de las áreas de dirección administrativa, dirección financiera y atención al usuario incluyendo personal de planta, funcionarios, contratistas y proveedores, también la Oficina de Control Interno del Concejo Distrital de Cartagena de Indias con el fin de que vele por el cumplimento de este

Directrices:

La Dirección Administrativa será vigilante del cumplimiento de las tareas de gestión de seguridad. Se realizará una definición de roles y responsabilidades que permita tener claridad acerca de las funciones que les corresponde a cada área.

Sin el compromiso de la alta dirección para que se realicen las tareas asignadas no se lograra el éxito en las tareas de seguridad asignadas.

9.1.1. Políticas que rigen para la estructura organizacional de seguridad de la información

- La Alta Dirección del Concejo Distrital de Cartagena de Indias debe aprobar los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo de acuerdo a lo establecido en la Guía 7 Roles y responsabilidades.

- La Alta Dirección del Concejo Distrital de Cartagena de Indias debe aprobar la conformación de un Comité de Seguridad de la Información.

- La Alta Dirección debe elaborar y aprobar un acta de compromiso donde manifieste su total apoyo a las actividades relacionadas con la seguridad de la información.

- La Alta Dirección debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este manual.

- La Alta Dirección debe promover activamente una cultura de seguridad de la información en la Institución.
- La Alta Dirección debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los servidores públicos, proveedores y partes interesadas de la entidad.

- La Alta Dirección del Concejo Distrital de Cartagena de Indias debe proveer todos los recursos necesarios para la gestión de la seguridad de la información de la entidad.

- El Comité de Seguridad de la Información debe revisar, periódicamente, las Políticas de Seguridad de la Información contenidas en el manual, la Metodología

para el Análisis de Riesgos de Seguridad y el Procedimiento para la Clasificación y Etiquetado de la Información, según lo considere pertinente.

- El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y realizar las gestiones pertinentes para la solución.

- El Comité de Seguridad de la Información debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

- El Responsable de Seguridad de la información será el líder del proyecto, escogido dentro comité de seguridad de la información y tendrá las siguientes responsabilidades
- Desarrollar los lineamientos para la gestión de la seguridad de la información del Concejo Distrital de Cartagena de Indias, estableciendo los controles que se obtengan del análisis de riesgo de seguridad realizado.

- Verificar el cumplimiento de los controles de seguridad de la información diseñados

- Definir los roles y responsabilidades del Concejo Distrital de Cartagena de Indias, así como socializarlos ante el Comité de Seguridad de la Información de la entidad, para su aprobación.

- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del sistema de seguridad y privacidad de la información.

- Verificar la permanencia del comité de seguridad de la información, proponer cambios, presentar la resolución de conformación del comité ante la alta dirección de la entidad.

Oficina de control interno:

Será la encargada de realizas las distintas auditorías internas al Modelo de seguridad y privacidad de la información con el fin de determinar si se están realizando adecuadamente los controles y si las distintas políticas de seguridad de la información se están cumpliendo.

La oficina de control interno presentara los respectivos hallazgos al área responsable y a la alta dirección con el fin de realizar las acciones correctivas y preventivas concernientes.

10. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN.

10.1. Política de Responsabilidad por los Activos.

Objetivo:

Garantizar que la información sea preservada con los principios de confidencialidad, integridad y disponibilidad al propietario de la información en las áreas de atención al usuario, dirección administrativa y dirección financiera del Concejo Distrital de Cartagena.

Alcance:

Comprende todo el personal desde la alta dirección hasta los colaboradores y custodios de los activos de los procesos de dirección administrativa, dirección financiera y atención al usuario incluyendo personal de planta, funcionarios, contratistas y proveedores, también la Oficina de Control Interno del Concejo Distrital de Cartagena de Indias con el fin de que vele por el cumplimento de este.

Directrices:

Los Propietarios de los Activos serán todos los líderes de los procesos, definidos y aprobados por la Alta Dirección de la entidad.

Identificación y clasificación de activos: La identificación de los activos de información se realizará anualmente con el fin de actualizar el inventario de activos, los Custodios de los Activos serán los líderes de áreas, de acuerdo a los procedimientos que señale La Dirección Administrativa de la entidad. Los propietarios de los activos de información realizaran esta actividad al interior de sus procesos al igual que la clasificación de los activos de información de acuerdo a la criticidad, sensibilidad y reserva de la misma.

Etiquetado de información: Todos los activos de información deberán ser rotulados y etiquetados por parte del propietario de este garantizando la confidencialidad, integridad

y disponibilidad de la información para esto se establecerá un procedimiento de etiquetado de información.

Devolución de activos: Una vez el propietario de la información cese sus actividades laborales con la empresa deberá entregar los activos físicos y de información a la entidad mediante un acta, con el fin de salvaguardar la información y los activos físicos de la entidad.

10.2. Políticas de responsabilidad por los activos

- Los Propietarios de los Activos monitorearan en forma periódica la validez de los usuarios y sus perfiles de acceso a la información.
- Los Propietarios de los Activos determinaran los criterios y niveles de acceso a la información.
- Los Propietarios de los Activos estarán sujetos a auditorias por parte de la oficina asesora de control interno del Concejo Distrital de Cartagena de Indias.
- Los Propietarios de los Activos recibirán los recursos tecnológicos asignados a sus funcionarios y contratistas, cuando estos cesan sus labores en la entidad o son transferidos a otras dependencias.
- El custodio de los activos verificara que los niveles de acceso a la información, definidos y aprobados por el propietario, se cumplan.
- El custodio de los activos comprobara que los accesos a archivos físicos, magnéticos u ópticos de información, sean los adecuados y aprobados por el propietario de la información.
- La Dirección Administrativa y el contratista de sistemas con la venia de la alta administración autorizaran la instalación, cambio o eliminación de componentes de la plataforma tecnológica de la entidad.
- El área de dirección administrativa con el contratista de sistema realizaran la configuración para el acceso a la información de contratistas, funcionarios, servidores públicos, y partes interesadas que requieran el acceso a los equipos tecnológicos y aplicaciones de información de la entidad.

- El área de dirección administrativa con el contratista de sistema prepara las estaciones de trabajo ya sea fijas o portátiles para entregar al custodio o propietario.
- Presidente, concejales y servidores públicos deben autorizar a sus funcionarios el uso de los recursos tecnológicos, previamente preparados por La Dirección Administrativa.
- Presidente, concejales y servidores públicos deben recibir los recursos tecnológicos asignados a sus colaboradores cuando estos se cesan sus actividades dentro de la entidad o los trasladan de dependencia.

11. POLÍTICA DE MANEJO DE MEDIOS.

Objetivo:

El Concejo Distrital de Cartagena de Indias debe garantizar y proveerá las condiciones de manejo de los tokens, periféricos o medio de almacenamiento de seguridad para los procesos y velará que hagan un uso responsable de estos.

Alcance:

Comprende todo el personal desde la alta dirección hasta los colaboradores y custodios de los activos de los procesos de dirección administrativa, dirección financiera y atención al usuario incluyendo personal de planta, funcionarios, contratistas y proveedores, también la Oficina de Control Interno del Concejo Distrital de Cartagena de Indias con el fin de que vele por el cumplimento de este

Directrices:

Es necesario establecer los usos y permisos que tienen los usuarios y/o funcionarios de la Entidad frente a los medios removibles como son el uso de tokens, periféricos y medios de almacenamiento en los equipos tecnológicos de la entidad a plataforma tecnológica de la entidad con el fin de reducir el riesgo de ataque malicioso, monitoreo de redes, etc.

11.1. Políticas para uso de tokens, periféricos o medio de almacenamiento de seguridad

- Es necesario que un solo funcionario sea asignado para la administración de tokens y autorizar el uso de estos u otro medio removible.
- El administrador de los tokens periféricos o medio de almacenamiento de seguridad debe autorizar el uso de tokens u otros medios removibles.
- El administrador de los tokens periféricos o medio de almacenamiento de seguridad debe recibirlos y activarlos de acuerdo a los procedimientos autorizados en los portales asignados.
- El administrador de los tokens periféricos o medio de almacenamiento de seguridad debe crear los perfiles y usuarios en los sitios web o portales para el uso de los tokens.
- El administrador de los tokens periféricos o medio de almacenamiento de seguridad debe entregar debidamente documentados (acta) los medios de almacenamiento o dispositivos a los funcionarios asignados con el respectivo usuario y serial del dispositivo.
- El administrador de los tokens periféricos o medio de almacenamiento de seguridad debe dar aviso a las entidades respectivas en el caso de pérdida o robo de los dispositivos o medios removibles.
- El administrador de los tokens periféricos o medio de almacenamiento de seguridad debe realizar el cambio respectivo una vez vencidos, presentan mal funcionamiento o se cambie el titular.
- Los Servidores públicos, funcionarios, Contratistas, Proveedores y Partes Interesadas deben cumplir la reglamentación en cuanto al uso de los dispositivos y medios periféricos, establecidos por La Dirección Administrativa y el Profesional de Seguridad de la Información del Concejo Distrital de Cartagena de Indias.
- Los Servidores públicos, funcionarios, Contratistas, Proveedores y Partes Interesadas no realizaran ningún tipo de modificación de la configuración realizada por La Dirección Administrativa.

- Servidores públicos, funcionarios, Contratistas, Proveedores y Partes Interesadas responsables de la custodia de los medios de almacenamiento y dispositivos asignados.
- Servidores públicos, funcionarios, Contratistas, Proveedores y Partes Interesadas no usaran medios removibles, ni dispositivos personales en los equipos tecnológicos de la entidad.

12. POLÍTICA DE CONTROL DE ACCESO.

12.1. Política de Acceso a Redes y Recursos de Red

Objetivo:

Garantizar que los usuarios que acceden a los recursos tecnológicos de la entidad y a las redes sigan lineamiento de seguridad que contribuyan a preservar la confidencialidad, integridad y disponibilidad de la información

Alcance:

Comprende todo el personal desde la alta dirección hasta los colaboradores y custodios de los activos de los procesos de dirección administrativa, dirección financiera y atención al usuario incluyendo personal de planta, funcionarios, contratistas y proveedores que necesiten acceder a las redes o a los recursos tecnológicos de la entidad. También la Oficina de Control Interno del Concejo Distrital de Cartagena de Indias con el fin de que vele por el cumplimento de esta.

12.2. Políticas de acceso a redes y recursos de red

- La Dirección Administrativa y el contratista encargado del área de sistemas deben garantizar que cada funcionario cuente con medios de autenticación para el acceso evitando accesos no autorizados.
- Se establecerán controles para identificar y autenticar a los usuarios en los recursos tecnológicos y redes de la entidad, cada usuario debe firmar un acta donde acepta la responsabilidad por el uso de usuario y contraseña.
- Para cualquier cambio en el acceso a los recursos tecnológicos en necesario solicitar autorización a La Dirección Administrativa- contratista de sistemas.
- Las contraseñas son personales e intransferibles no pueden compartirse cualquier manejo inadecuado de usuarios y contraseñas, las consecuencias legales recaen sobre el usuario principal

- El Profesional de Seguridad de la Información verificara en forma periódica debe verificar en forma periódica los periódicamente los controles de acceso para los diferentes usuarios velando que estén las restricciones necesarias de acuerdo al perfil generado.
- Todos los servidores públicos, funcionarios, contratistas y partes interesadas deben solicitar a La Dirección Administrativa por primera vez la creación de usuario, contraseña y firma del acta de compromiso para el cumplimiento de las políticas de seguridad de la entidad.

12.3. Política de administración de acceso de usuarios.

Objetivo:

Garantizar que todas las dependencias del Concejo Distrital de Cartagena administren los usuarios autenticados en los recursos tecnológicos y sistemas de información del Concejo Distrital de Cartagena de Indias.

Alcance:

Comprende La Dirección Administrativa- contratista de sistemas, Profesional de Seguridad de la Información, Propietarios de la Información y Custodios de la Información.

12.3.1. Políticas de administración de acceso de usuarios

- El Presidente, los concejales y servidores públicos deben solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario, para los funcionarios que laboran en sus áreas, acogiéndose al procedimiento establecidos para tal fin.
- La Dirección Administrativa a través del contratista de sistema debe administrar adecuadamente los usuarios de las redes, sistemas de información y recursos

tecnológicos de la entidad esto incluye: creación, eliminación, bloqueo, restricciones y modificaciones.

- La Dirección Administrativa a través del contratista de sistemas establecerá el procedimiento para el acceso a los diferentes recursos tecnológicos de la entidad.
- Los propietarios de los activos de información serán los responsables de, definir los perfiles de usuario y autorizar con La Dirección Administrativa las solicitudes de acceso a los recursos tecnológicos de acuerdo con los perfiles establecidos.
- Los propietarios de los activos de información deberán verificar y ratificar en forma periódica las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

.

13. POLÍTICAS DE CRIPTOGRAFÍA.

Objetivo:

Velar porque la información clasificada como restringida del Concejo Distrital de Cartagena de Indias se cifre en el momento del almacenarse o transmitirse por cualquier medio.

Alcance:

Comprende La Dirección Administrativa – sistemas y para los que desarrollen sistemas de información solicitados por la entidad.

Directrices:

- Contar con el inventario de activos de información clasificado y etiquetado.

13.1. Políticas de controles criptográficos

- La Dirección Administrativa - contratista de sistema deberá almacenar y/o transmitir, la información digital, etiquetada como reservada en forma cifrada en aras de proteger la confidencialidad e integridad.

- La Dirección Administrativa - contratista de sistema verificara que los sistemas de información o aplicativos que se vayan a almacenar o transmitir tengan mecanismos de cifrado de datos.

- La Dirección Administrativa - contratista de sistema implementara estándares mínimos para aplicar controles informáticos.

- Si se desarrollan nuevos sistemas de información para el Concejo se garantizará la confiabilidad de los sistemas de almacenamientos, para la información reservada, cumpliendo los estándares establecidos por La Dirección Administrativa- contratista de sistemas.

14. POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO.

Objetivo:

Garantizar que los servidores públicos, funcionarios, contratistas, proveedores, partes interesadas, ciudadano y/o visitante, que utilice las instalaciones físicas del Concejo Distrital de Cartagena de Indias, realice su ingreso y salida, cumpliendo con los lineamientos de seguridad física adecuados y aprobados por la alta dirección de la entidad.

Alcance:

Comprende todos los usuarios, ciudadanos, visitantes, alta dirección, proveedores, funcionarios, contratistas y partes interesadas que hagan uso de las instalaciones físicas del Concejo Distrital de Cartagena.

14.1. Políticas de áreas seguras

- La Dirección Administrativa realizará las autorizaciones para las diferentes áreas de la entidad, para las áreas sensibles, los visitantes, contratistas deberán estar acompañados por el funcionario autorizado.
- La Dirección Administrativa a través de un funcionario asignado registrara el ingreso de visitantes.
- Se restringirá el acceso a las áreas sensibles de la infraestructura física de la entidad a los contratistas o funcionarios que estén desvinculados laboralmente o en licencia y/o vacaciones.
- La Dirección Administrativa será vigilante de proveer las condiciones medioambientales y físicas para proteger los recursos tecnológicos de la entidad, proveyendo los sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones

ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

- La Dirección Administrativa protegerá los recursos tecnológicos contra fallas e interrupciones eléctricas, además separara estos de líquidos inflamables, el mantenimiento de las redes eléctricas, de voz y datos se realizará por personal idóneo, certificado y se programaran mantenimientos preventivos.
- La alta dirección controlara el acceso físico, del personal que labora en las áreas de la entidad.
- El presidente, los concejales y servidores públicos que se encuentren en áreas restringidas deben velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en su área.
- Presidente, Concejales y servidores públicos que se encuentren en áreas restringidas deben autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso a sus áreas.
- Todos los servidores públicos, proveedores, ciudadanos y/o visitantes, deben hacer uso del sistema de control de acceso, para ingresar y salir de las instalaciones físicas de la entidad.
- Todos los servidores públicos, proveedores, ciudadanos y/o visitantes deben portar el carnet, que los identifica como tales, además de usar las prendas distintivas que faciliten su identificación.

15. POLÍTICAS DE SEGURIDAD DE LAS OPERACIONES.

Objetivo:

Elaborar, revisar y aprobar la documentación concerniente a la plataforma tecnológica que utilice el Concejo Distrital de Cartagena de Indias cumpliendo con las responsabilidades operativas que se le asignen a cada servidor público de Dirección administrativa- Sistemas.

Alcance:

Comprende el área de Dirección administrativa – Sistemas del Concejo Distrital de Cartagena.

Directrices:

- Contar con los instructivos, guías y manuales de los recursos y servicios tecnológicos necesarios para la oración de la entidad.

15.1. Política de Asignación de Responsabilidades Operativas.

- La Dirección Administrativa- contratista de sistemas realizara y aprobara la documentación necesaria para la administración y operación de la plataforma tecnológica de la entidad.

- La Dirección Administrativa- contratista de sistemas entregará a los servidores públicos las guías, manuales o instructivos de operación y/o configuración de los sistemas operativos para servidores, actualización de servidores, servicios de red, Backus, y sistemas de información que conforman la plataforma tecnológica de la entidad.

- El Profesional de Seguridad de la Información asesora, emitirá y generará recomendaciones de seguridad, a las propuestas realizadas por La Dirección Administrativa- contratista de sistemas, para la plataforma tecnológica del Concejo Distrital de Cartagena.
- El Profesional de Seguridad de la Información realizará monitoreo periódicamente a las actividades de clasificación y etiquetado de los documentos de administración y operación de la plataforma tecnológica de la entidad.
- El Profesional de Seguridad de la Información monitoreara en forma periódica la seguridad de los espacios usados para almacenar la documentación de operación y administración, de la plataforma tecnológica del Concejo Distrital de Cartagena.

15.2- Política de Protección Contra Códigos Maliciosos.

Objetivo:

Garantizar y proporcionar al Concejo Distrital de Cartagena de Indias herramientas que protejan la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente que puedan ser causados software malicioso.

Alcance:

Comprende la Dirección Administrativa- Contratista de Sistema y todos los funcionarios, servidores públicos, contratistas, proveedores e interesados que utilicen las herramientas informáticas del Concejo Distrital de Cartagena

Directrices:

Con el fin de cumplir con esta política es necesario contar con software antivirus, antimalware, anti spam y antispyware licenciados, instalados y configurados en todos los equipos informáticos de la entidad.

15.2.1. Políticas de protección frente a software malicioso

- La Dirección Administrativa- contratista de sistemas suministrara las herramientas que permitirán resguardar a la entidad contra los softwares maliciosos, herramientas como antivirus, antimalware, anti spam, antispyware y así mitigar el riesgo de infección del os equipos de la entidad protegiendo la seguridad de la información de la plataforma tecnológica del Concejo Distrital de Cartagena y los servicios que se prestan.
- La Dirección Administrativa- contratista de sistemas se asegurará que el software de antivirus, antimalware, anti spam y antispyware esté debidamente licenciado con el fin de que se pueda actualizar periódicamente.
- La Dirección Administrativa- contratista de sistemas certificará que la información que esta almacenada en los equipos informáticos de la entidad y en la plataforma tecnológica esta escaneada por el software de antivirus, esto incluye la información que se transmite por correo electrónico.
- Los servidores públicos, contratistas, proveedores y partes interesadas no podrán realizar ningún tipo de cambio en la configuración del software de antivirus, antispyware, antimalware, anti spam, definidas por La Dirección Administrativa-contratista de sistemas; solo están autorizados a escanear los diferentes medios de almacenamiento.
- Los servidores públicos, contratistas, proveedores y partes interesadas realizaran el escaneo de los diferentes archivos o documentos usados por primera vez a través de la ejecución del software de antivirus, antispyware, anti spam, antimalware.
- Los servidores públicos, contratistas, proveedores y partes interesadas se asegurarán que los archivos adjuntos (documentos, fotos, etc.) procedentes de correos electrónicos o de cualquier medio de almacenamiento externo, provienen de fuentes conocidas y seguras, para evitar la infección de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos de la entidad.

- Los servidores públicos, contratistas, proveedores y partes interesadas al detectar o sospechar de algún virus o software malicioso notificaran a la Dirección Administrativa- contratista de sistemas con el fin de tomar las medidas de control correspondientes.

15.3. Política de copias de respaldo de la información

Objetivo:

Certificar la realización de copias de respaldo y almacenamiento de la información relevante de la entidad, facilitando las herramientas necesarias y creando los procedimientos y mecanismos para el cumplimiento de estas tareas.

Alcance:

Comprende la Dirección Administrativa- Contratista de Sistema y todos los funcionarios, servidores públicos, contratistas, proveedores e interesados que utilicen las herramientas informáticas del Concejo Distrital de Cartagena

Directrices:

Diseñar los procedimientos de copias de respaldo y recuperación de la información del Concejo Distrital de Cartagena, poseer la tecnología adecuada para el almacenamiento de la información de las copias que se guarden.

15.3.1. Políticas de copias de respaldo de la información

- La Dirección Administrativa- contratista de sistemas, en compañía del Profesional de Seguridad de la Información elaboraran los diferentes procedimientos para la ejecución y restauración de las copias de respaldo de la información.
- La Dirección Administrativa- contratista de sistemas dispondrán las diferentes herramientas tecnológicas que permitirán disponer de los medios de almacenamiento que soporte las copias de seguridad de la información que se realicen.
- La Dirección Administrativa- contratista de sistemas definirá la estructura organizacional de directorios de respaldo y estrategia de retención y rotación, de las copias de respaldo de la información de la entidad.
- La Dirección Administrativa- contratista de sistemas definirá y aprobara los tiempos en que se realizaran las actividades de copia de respaldo y restauración de la información de la entidad
- El Profesional de Seguridad de la Información monitoreara en forma periódica que se cumplan las actividades de generación de copias de respaldo de la información de la entidad y la restauración de la misma, para verificar el estado en que se encuentra.

16. POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES.

Objetivo:

Garantizar que el acceso a la red institucional tenga los lineamientos y controles de seguridad, que impidan que personal no autorizado, conecten equipos en la LAN de la entidad para fines no establecidos.

Alcance:

Comprende la Dirección Administrativa- Contratista de Sistema, además por el Profesional de Seguridad de la Información.

Directrices:

Identificar las herramientas tecnológicas y servicios de la red de la entidad, contar con un servicio de protección perimetral, configurado en alta disponibilidad que permita cumplir la política.

16.1. Políticas de gestión y aseguramiento de las redes de datos

- La Dirección Administrativa- contratista de sistemas tomará las medidas que permitan asegurar la disponibilidad de los recursos tecnológicos y servicios de red de la entidad.
- La Dirección Administrativa- contratista de sistemas diseñara e implantara controles, que permitan reducir los riesgos de seguridad de la información, que proviene de las redes de datos de la entidad
- La Dirección Administrativa- contratista de sistemas mantendrá las redes de datos, segmentadas de acuerdo a los tipos que considere y que le permitan una configuración adecuada de los dispositivos de seguridad perimetral de la red.

- La Dirección Administrativa- contratista de sistemas realizara la documentación de los servicios, protocolos y puertos de comunicación, autorizados en las redes de datos e inhabilitará o eliminará los servicios, protocolos y puertos que no se utilicen o que constituyan un riesgo en su operación.
- La Dirección Administrativa- contratista de sistemas realizara la definición de los mecanismos de protección entre las redes internas de la entidad y cualquier red externa.
- La Dirección Administrativa- contratista de sistemas preservara debidamente la confidencialidad de la información relacionada con el direccionamiento IP y enrutamiento de paquetes, desde la LAN de la entidad, hacia y desde el exterior.

16.2. Política de uso del Correo Electrónico

Objetivo:

El Concejo Distrital de Cartagena de Indias, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico.

Alcance:

Será aplicada por La Dirección Administrativa- contratista de sistemas, además por el Profesional de Seguridad de la Información y Los servidores públicos, contratistas, proveedores y partes interesadas de la entidad.

Directrices:

Con el fin de dar cumplimiento a esta política es necesario diseñar y aprobar el procedimiento para crear las cuentas de correo electrónico de la entidad.

16.2.1. Políticas de uso del correo electrónico

- La Dirección Administrativa- contratista de sistemas diseñará y aprobará el Procedimiento para crear las Cuentas de Correo Electrónico.
- La Dirección Administrativa- contratista de sistemas dará los lineamientos para el uso del correo electrónico.
- La Dirección Administrativa- contratista de sistemas proveerá un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
- Los servidores públicos, contratistas, proveedores y partes interesadas entenderá que la cuenta de correo electrónico creado y asignado, es para uso individual; este será de carácter institucional y para el desempeño de sus funciones en la entidad, por lo tanto la información y mensajería que contenga son de propiedad del Concejo Distrital de Cartagena, es necesario que se abstengan de enviar mensajes que cualquier índole diferente a las funciones y servicios que presta el Concejo Distrital de Cartagena.
- El Profesional de Seguridad de la Información revisara en forma periódica los lineamientos definidos por La Dirección Administrativa- contratista de sistemas para el uso del correo electrónico.

16.3. Política de uso adecuado de internet

Objetivo:

Suministrar los recursos que permitan asegurar la disponibilidad a los usuarios que requieran de Internet para el desempeño de sus funciones.

Alcance:

Será aplicada por La Dirección Administrativa- contratista de sistemas, además por el Profesional de Seguridad de la Información y Los servidores públicos, contratistas, proveedores y partes interesadas de la entidad.

Directrices:

Contar con un canal de Internet en operación con el fin de cumplir la política de uso adecuado del Internet.

16.3.1. Políticas de uso adecuado de internet

- La Dirección Administrativa- contratista de sistemas suministrara los recursos tecnológicos y humanos, necesarios para la implementación, administración y mantenimiento, requeridos para la prestación segura del servicio de Internet.
- La Dirección Administrativa- contratista de sistemas monitoreara en forma permanente el canal de servicio de Internet adquirido.
- La Dirección Administrativa- contratista de sistemas diseñará procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios que se cataloguen como restringidos.
- La Dirección Administrativa- contratista de sistemas realizará los registros de la navegación y los accesos de los usuarios a Internet.

- Los servidores públicos, contratistas, proveedores y partes interesadas deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
- Los servidores públicos, contratistas, proveedores y partes interesadas evitaran descargar software desde el internet institucional, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
- Los servidores públicos, contratistas, proveedores y partes interesadas no deben acceder a páginas relacionadas con pornografía, drogas, alcohol, web proxys, hacking

16.4. Política de intercambio de información

Objetivo:

Garantizar la protección de la información que se transfiera hacia tercero que la solicite, cumpliendo con los controles y procedimientos que garanticen la confidencialidad, preservación e integridad de los datos del Concejo Distrital de Cartagena.

Alcance:

Comprende la Dirección Administrativa- Contratista de Sistema y todos los funcionarios, servidores públicos, contratistas, proveedores e interesados que utilicen las herramientas informáticas del Concejo Distrital de Cartagena

Directrices:

Contar con un Procedimiento de Intercambio de Información Física y un Procedimiento de Intercambio de Información Digital para la entidad aprobado.

16.4.1. Políticas de intercambio de información

- La Oficina Asesora Jurídica definirá el modelo de Acta / acuerdo o compromiso de confidencialidad para los contratistas de la entidad, incluyendo los compromisos adquiridos y las penalidades para el incumplimiento de dicho acuerdo.
- La Oficina Asesora Jurídica debe incluir el Acuerdo y/o Cláusula de Confidencialidad en los contratos, cuando el interventor de Contrato lo solicite, mediante el documento de estudios previos
- El interventor de Contrato solicitara la inclusión en los contratos el Acuerdo y/o Cláusula de Confidencialidad.
- El Profesional de Seguridad de la Información elaborará el Procedimiento de Intercambio de Información Física y el Procedimiento de Intercambio de Información Digital para la entidad
- El servidor público de correspondencia usara el Procedimiento de Intercambio de Información Física con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.
- La Dirección Administrativa- contratista de sistemas brindara las herramientas de intercambio de información seguros, así como adoptara controles como el cifrado de información, que permitan el cumplimiento del Procedimiento para el Intercambio de Información Digital, con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.
- Los Terceros con quienes se intercambia información de la entidad darán un manejo adecuado a la información recibida, en cumplimiento de las Políticas de Seguridad del Concejo Distrital de Cartagena, las políticas aprobadas y los acuerdos de confidencialidad firmados.
- Los servidores públicos, partes interesadas no deben intercambiar información sensible de la entidad por vía telefónica.

17. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

17.1. Política para el establecimiento de requisitos de seguridad

Objetivo:

Certificar que el software y todos los servicios TIC que adquiere el Concejo Distrital de Cartagena de Indias cumplan con los requisitos de seguridad y calidad establecidos por él.

Alcance:

Comprende la Dirección Administrativa- Contratista de Sistema y todos los funcionarios, servidores públicos, contratistas, proveedores e interesados que utilicen las herramientas informáticas del Concejo Distrital de Cartagena.

Directrices:

Con el fin de dar cumplimiento a la Política para el establecimiento de requisitos de seguridad de los sistemas de información de la entidad, es perentorio contar con un procedimiento para adquisición del software y servicios TIC.

17.1.1. Políticas para el establecimiento de requisitos de seguridad

- La Dirección Administrativa- contratista de sistemas definirá los custodios de los sistemas de información de la entidad, bajo su responsabilidad.

- La Dirección Administrativa- contratista de sistemas definiera los protocolos para la adquisición de los sistemas de información de la entidad.

- La Dirección Administrativa- contratista de sistemas documentara los requerimientos establecidos y definirá la arquitectura de software más

conveniente para cada sistema de información que se requiera de acuerdo con los requerimientos de seguridad y los controles definidos, asegurando que este utilice herramientas licenciadas en el mercado.

17.2. Política de desarrollo seguro, realización de pruebas y Soporte de los sistemas

Objetivo:

Garantizar que los sistemas de información del Concejo Distrital de Cartagena de Indias cuenten con los lineamientos de seguridad y soporte que permitan garantice la preservación de la confidencialidad, integridad y disponibilidad de los datos institucionales, soportados en los aplicativos de la entidad.

Alcance:

Comprende la Dirección Administrativa- Contratista de Sistema y el profesional de seguridad de la información del Concejo Distrital de Cartagena.

Directrices:

Contar con un procedimiento para desarrollar pruebas al software adquirido por la entidad

17.2.1. Normas de desarrollo seguro, realización de pruebas y soporte de los sistemas

- Los responsables de los Sistemas de Información de la entidad realizarán las pruebas necesarias que permitan asegurar que los programas o aplicativos de información institucionales cumplen con los requerimientos de seguridad establecidos.

- La Dirección Administrativa- contratista de sistemas controlará las versiones de los sistemas de información de la entidad, para de esta manera, garantizar buenas prácticas en la administración de los cambios propuestos y aprobados.

- La Dirección Administrativa- contratista de sistemas verificara que los sistemas de información adquiridos estén debidamente licenciados y con los derechos de propiedad intelectual.

- El profesional de seguridad de la información realizara las pruebas de seguridad, eficiencia y otras que permitan verificar la eficiencia del software adquirido.

18. POLÍTICAS DE RELACIONES CON LOS PROVEEDORES.

18.1. Política de Seguridad de la Información en las Relaciones con los Proveedores.

Objetivo:

Garantizar que el Concejo Distrital de Cartagena mantenga buenas relaciones con los proveedores o terceros cumpliendo los lineamientos de seguridad de la información preservando la confidencialidad, integridad y disponibilidad de los datos.

Alcance:

Comprende la Oficina Asesora Jurídica, Dirección Administrativa, los interventores de los contratistas y el Profesional de Seguridad de la Información.

Directrices:

Contar dentro del contrato con una Cláusula y/o Acuerdo de Confidencialidad y la Cláusula y/o Acuerdo de Aceptación de las Políticas de Seguridad de la Información para la entidad.

18.1.1. Normas de inclusión de condiciones de seguridad en la relación con terceras partes

- La Oficina Asesora Jurídica incluirá en el estudio previo, las Obligaciones del Contratista (en cuanto al servicio que va a prestar), la Cláusula y/o Acuerdo de Confidencialidad y la Cláusula y/o Acuerdo de Aceptación de las Políticas de Seguridad de la Información para la entidad.
- Los interventores de contratos divulgarán las políticas y procedimientos de seguridad de la información del Concejo.

- La Dirección Administrativa- contratista de sistemas establecerá las condiciones de conexión adecuada, para los equipos de cómputo y dispositivos móviles de los proveedores o terceros, en la red de datos.
- La Dirección Administrativa- contratista de sistemas establecerá las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros o proveedores de servicios.
- La Dirección Administrativa- contratista de sistemas mitigará los riesgos relacionados con terceras partes o proveedores, que tengan acceso a los sistemas de información y los recursos tecnológicos de la entidad.
- El Profesional de Seguridad de la información realizará la identificación y monitoreo de los riesgos relacionados con proveedores y terceras partes o los servicios provistos por ellas.

19. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

19.1- Política de Gestión de Incidentes y Mejoras en la Seguridad de la Información.

Objetivo:

Garantizar una adecuada gestión de incidentes de seguridad que permita mitigar los riesgos que afectan la preservación de la confidencialidad, integridad y disponibilidad de la información.

Alcance:

Comprende la Dirección Administrativa- contratista de sistemas, los custodios de la Información y servidores públicos, partes interesadas y proveedores de la entidad.

Directrices:

Contar con la documentación de los incidentes de seguridad y los tratamientos que se han realizado para así poder realizar una administración adecuada de estos.

19.1.1. Políticas para el reporte y tratamiento de incidentes de seguridad

- Todos los servidores públicos, contratistas, proveedores y partes interesadas realizarán el reporte de cualquier incidente o evento relacionado con la información y/o los recursos tecnológicos de la entidad en forma inmediata.
- Los servidores públicos, contratistas, proveedores y partes interesadas notificarán en forma inmediata a su jefe o interventor del contrato la pérdida o divulgación de información confidencial para que se registre y se le dé el tratamiento adecuado al caso.

- La Dirección Administrativa- contratista de sistemas proveerá una respuesta oportuna frente a los incidentes de seguridad de la información identificados y reportados.
- La Dirección Administrativa- contratista de sistemas realizará evaluación a cada uno de los incidentes de seguridad que se presenten e informará al Profesional de Seguridad de la Información sobre el tema.
- La Dirección Administrativa- contratista de sistemas realizara la designación de personal calificado, para investigar exhaustivamente los incidentes de seguridad reportados, identificando las causas, proporcionando las soluciones y finalmente previniendo su aparición nuevamente, creando un repositorio de conocimiento que reduzca el tiempo de respuesta para los incidentes futuro.

20. POLÍTICAS DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO.

20.1- Política de Continuidad de Seguridad de la Información.

Objetivo:

Proporcionar las herramientas que permitan dar una respuesta adecuada por parte de los funcionarios del Concejo Distrito de Cartagena de Indias en caso de contingencia o eventos catastróficos que se presenten y que afecten la continuidad de su operación.

Alcance:

Comprende la Alta Dirección, Dirección Administrativa, además por el Profesional de Seguridad de la Información.

Directrices:

Aprobar y elaborar procedimientos de Contingencia, Recuperación y Retorno a la Normalidad.

20.1.1. Políticas de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

- La Alta Dirección, el Profesional de Seguridad de la Información, La Dirección Administrativa- contratista de sistemas, identificará los escenarios que se puedan presentar como emergencia o desastre, los procesos y/o las áreas que la componen, la infraestructura tecnológica en general y definir cómo se debe actuar ante la presencia de dichos desastres.
- La Alta Dirección, el Profesional de Seguridad de la Información, La Dirección Administrativa- contratista de sistemas, liderarán los temas relacionados con la continuidad del negocio y la recuperación ante cualquier tipo de desastre.

- La Alta Dirección, el Profesional de Seguridad de la Información, La Dirección Administrativa- contratista de sistemas, diseñará las estrategias de recuperación adecuadas para la entidad.
- La Alta Dirección, el Profesional de Seguridad de la Información, La Dirección Administrativa- contratista de sistemas, asegurarán la realización de las pruebas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y documentando el resultado de dichas pruebas.
- El Profesional de Seguridad de la Información ejecutará los análisis de impacto al negocio y los análisis de riesgos de continuidad para proponer posibles estrategias de recuperación, en caso de activarse el plan de contingencia o continuidad del negocio, con las consideraciones de seguridad de la información a que sean pertinentes tener en cuenta.
- El Profesional de Seguridad de la Información certificará que los Procedimientos de Contingencia, Recuperación y Retorno a la Normalidad, incluyan las consideraciones de seguridad de la información necesaria y requerida, para el cumplimiento de los objetivos trazados.

20.2. Política de redundancia

Objetivo:

Propender porque exista una plataforma tecnología cuente con una solución redundante en su operación, para beneficiar la preservación de la disponibilidad en su funcionamiento.

Alcance:

Comprende La Dirección Administrativa- contratista de sistemas y el profesional de Seguridad de la Información.

Directrices:

Tener identificado los sistemas de información, servicios y recursos tecnológicos que contribuyen al cumplimiento de los objetivos y misión de la entidad que permitan cumplir con la política de redundancia.

20.2.1. Políticas de redundancia

- La Dirección Administrativa- contratista de sistemas, junto con el Profesional de Seguridad de la Información de la entidad, realizará el análisis, identificación y definición de los requerimientos de redundancia para los sistemas de información, servicios y recursos tecnológicos de la entidad, clasificados como críticos.
- La Dirección Administrativa- contratista de sistemas junto con el Profesional de Seguridad de la Información de la entidad realizara la evaluación, definición de soluciones de redundancia para los sistemas de información, servicios y recursos tecnológicos, clasificados como críticos**.**
- La Dirección Administrativa- contratista de sistemas administrará las soluciones de redundancia tecnológica de la entidad y realizará pruebas periódicas a dichas soluciones.

21. POLÍTICAS DE CUMPLIMIENTO.

21.1. Política de Cumplimiento de Requisitos Legales y Contractuales

Objetivo:

Velar por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información del Concejo Distrital de Cartagena de Indias , tales como derechos de autor y propiedad intelectual del software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

Alcance:

Será aplicada por La Dirección Administrativa- contratista de sistemas, además por todos los servidores públicos, partes interesadas y proveedores de la entidad.

21.1.1. Políticas de cumplimiento con requisitos legales y contractuales

- La Dirección Administrativa- contratista de sistemas garantizara que el software instalado en la plataforma tecnológica de la entidad, esté protegido por derechos de autor y requiera licencia de uso.
- La Dirección Administrativa- contratista de sistemas realizará un inventario con el software y sistemas de información, autorizados a operar en las estaciones de trabajo o equipos móviles de la entidad.
- Todos los servidores públicos, contratistas, partes interesadas y proveedores no instalarán software o sistemas de información en las estaciones de trabajo o equipos móviles suministrados por la entidad para el desarrollo de sus funciones.
- Todos los servidores públicos, contratistas, partes interesadas y proveedores cumplirán con las leyes de derechos de autor y acuerdos de licenciamiento de software.

21. 2. Política de privacidad y protección de datos personales

Objetivo:

Garantizar que los datos personales almacenados en los sistemas de información, repositorios y recursos informáticos del Concejo Distrital de Cartagena de Indias, reciban una protección óptima, para preservar la confidencialidad, integridad y disponibilidad de los mismos.

Alcance

Comprende la Dirección Administrativa – Contratista de Sistema y todas las áreas que manejen datos personales.

Directrices:

Identificar los sistemas de información, repositorios y recursos informáticos que almacenan, recolectan y procesan datos personales, para fines de la entidad.

21.2.1. Políticas de privacidad y protección de datos personales

- Las distintas dependencias que procesan datos personales de servidores públicos, contratista, proveedores y partes interesadas, tendrán que obtener la autorización para el tratamiento de estos datos, con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir, dichos datos personales en el desarrollo de las funciones propias de la entidad.
- Las distintas dependencias que procesan datos personales de servidores públicos, contratista, proveedores y partes interesadas asegurarán que solo las personas que necesiten los datos en forma legítima, de acuerdo a sus funciones y responsabilidades, puedan tener acceso a dichos datos.
- Las distintas dependencias que procesan datos personales de servidores públicos, contratista, proveedores y partes interesadas cumplirán con las normas técnicas establecidas para enviar datos personales a los propietarios, mediante el correo electrónico y/o mensajes de texto.

22. CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS