PLAN TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Personería Distrital de Cartagena de Indias 2024

PERSONERÍA AUXILIAR

PERSONERIA
DE CARTAGENA DE INDIAS

INTRODUCCION

El presente Plan de Tratamiento de Riesgos se elabora con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno digital en el Eje Temático de la Estrategia en **seguridad y privacidad de la información**, el cual busca proteger los datos de los ciudadanos garantizando la seguridad de la información.

OBJETIVOS

Aplicar el plan de acción a los procesos existentes de la Personería Distrital de Cartagena de Indias con el fin de proteger los activos de información, el manejo de medios, el control de acceso y la gestión de los usuarios.

OBJETIVOS ESPECIFICOS

- Elaborar un plan de trabajo para la implementación del plan de tratamiento de riesgode seguridad y privacidad de la información.
- Aplicar en cada uno de los procesos la metodología para la aplicación en los diferentes procesos.

ALCANCE

La Personería Distrital de Cartagena es una entidad orientada al mejoramiento continuo, a través de su plan de acción de tratamiento de riesgode seguridad y privacidad de la información, se aplicara a todas las áreas de la entidad, con el compromiso día a día en la satisfacción de las necesidades de sus usuarios (comunidad) a través de la prestación de servicios de calidad, atendidos oportunamente y con respeto a la dignidad humana, enmarcados en los parámetros de ley; los cuales se soportan en procesos óptimos, un equipo de colaboradores competentes y en mecanismos de comunicación efectivos.

TERMINOS Y DEFINICIONES

Activo de información: Todo aquello que tiene valor para la entidad y por lo tanto debe protegerse.De acuerdo con la norma ISO 27001 los activos de información se clasifican en: información, software, activos físicos, personas, servicios e intangibles como reputación, imagen de la entidad, etc.

Borrado seguro: procedimiento de eliminación de archivos que no permite la recuperación posteriorde éstos.

Centro de Servicios Informáticos - CSI: equipo responsable de gestionar las solicitudes de servicio relacionadas con las plataformas de tecnologías de información de la Personería Distrital de Cartagena de Indias.

Confidencialidad: Garantizar el necesario nivel de secreto de la información y de su tratamiento, para prevenir su divulgación no autorizada cuando está almacenada o en tránsito.

Correo masivo: expresión usada en el presente manual de políticas para referirse a mensajes de correo electrónico enviado a 100 o más destinatarios que no formen parte de los dominios de la Personería Distrital de Cartagena de Indias.

Criterio de seguridad de la información de la Personería Distrital de Cartagena de Indias: conjunto de requisitos técnicos que deben considerarse para la planeación e implementación segura de infraestructura y aplicaciones de tecnología de información, así como para su posterior verificación.

Custodio de la información: es el usuario de la información que ejerza funciones de administraciónde sistemas de información. Sus responsabilidades incluyen: Garantizar que se cumplan los nivelesde servicio definidos.

Proporcionar asistencia al dueño de la información en la selección desoluciones técnicas apropiadas. Proveer operativamente el aseguramiento de la confidencialidad, integridad y disponibilidad de la información.

Derechos / Privilegios de acceso: conjunto de permisos dados a un usuario o a un sistema para acceder a un determinado recurso (repositorio información, aplicativo, datos).

Disponibilidad: La información estará lista para acceder a ella o utilizarse cuando se necesite.

Dueño de activo de información: (o propietario). Servidor público de nivel directivo cuyo rol implica entender qué tipo de información es mantenida, creada, procesada o eliminada; cómo la informaciónse desplaza en su área de responsabilidad y quien debe acceder a la información y por qué. Como resultado, son capaces de entender e identificar los riesgos a la información. Tiene la responsabilidad de asegurar la Clasificación de los activos y tomar decisiones sobre estos (por ejemplo: ubicación, acceso y controles de seguridad).

Entidad: término que se usa en el presente documento para identificar a la Personería Distrital de Cartagena de Indias. Cuando sea conveniente. Equipos de trabajo de informática: equipos de trabajode la Personería Distrital de Cartagena de Indias que son responsables de desarrollar, desplegar, mantener, proteger y administrar las plataformas de tecnología de información.

Evento de seguridad de la información: Presencia identificada del estado de un sistema, servicio o red, que indica una posible violación de las políticas de seguridad de la información, una falla de los controles, o una situación desconocida previamente que puede ser relevante para la seguridad.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. Todo incidente es un evento,más no todo evento es un incidente.

Integridad: La información debe estar completa y correcta en todo momento

Plataforma de tecnologías de información / Plataforma de T.I.C.:

Para propósitos del presente documento, las expresiones “plataforma de T.I.” y “plataforma de tecnologías de Información” hace referencia a todo el conjunto de recursos de tecnología de la información usados para generar, procesar, almacenar y transmitir información de la Personería Distrital de Cartagena de Indias. Lo que incluye por ejemplo: sistemas de información, equipos de escritorio, portátiles, sistemas

operativos e infraestructura de red.

Seguridad de la información:
Preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguridad informática: Rama de la seguridad de la información que se enfoca en la protección dela plataforma de tecnología de Información y de los datos que circulan, se procesan o almacenan endicha plataforma.

Servidores Públicos: Término que se usa en el presente documento para identificar a empleados públicos, trabajadores oficiales y practicantes de la Personería Distrital de Cartagena de Indias.

Sistema de Gestión de Seguridad de la Información - SGSI: Sistema de gestión basado en un enfoque hacia los riesgos, cuyo fin es establecer, implementar, operar, Hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. El SGSI se rige por los requisitos de la norma internacional de gestión ISO/IEC 27001.

Software malicioso: (También, código malicioso). Es un tipo de software que tiene como objetivo infiltrar o dañar un equipo de cómputo o sistema de información sin el consentimiento de su propietario. El software malicioso incluye virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo y crimeware. El término “software malicioso” también hace referencia a software hostil o molesto.

Usuario: Persona, proceso o aplicación de la entidad autorizada para acceder a la información de entidad o a los sistemas que la manejan.

Zonas restringidas de procesamiento: Son áreas, recintos o edificaciones ubicadas dentro de lassedes de la Personería Distrital de Cartagena de Indias, destinadas a alojar Plataformas detecnología de la información, recursos importantes o información de la entidad; razón por la que requieren controles especiales de seguridad física y control de acceso.

MARCO NORMATIVO

Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídicotutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entreotras disposiciones".

Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales". Reglamentada parcialmente por el Decreto Nacional 1377 de 2013.

Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones". Reglamentada parcialmente por el Decreto Nacional 103 de 2015.

Decreto Nacional 2573 de 2014 "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".

Decreto 1078 del 26 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

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

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La información es un activo estratégico para las operaciones diarias de la Personería Distrital y a su vez un factor determinante para el éxito de su plan de desarrollo. Por ello, la entidad está comprometida con la adopción de buenas prácticas de seguridad de la información tendientes a implementar, mantener y mejorar su Sistema de Gestión de Seguridad de la Información SGSI. Las Políticas y lineamientos de Seguridad de la Información y de las TI son de carácter obligatorio y deben ser conocidas y cumplidas por los servidores públicos, proveedores, contratistas y usuarios externos que hagan uso de la información y de los recursos tecnológicos de la entidad.

POLÍTICAS PARA SERVIDORES PÚBLICOS Y CONTRATISTAS EXTERNOS

Estas políticas aplican tanto a los procesos realizados directamente por la Personería Distrital de Cartagena de Indias, como a los ejecutados a través de contratos o acuerdos con terceros. Deben ser conocidas y cumplidas por los servidores públicos, proveedores, contratistas y usuarios externosde la entidad y de las sedes externas de la entidad que hagan uso de la información institucional y de sus recursos tecnológicos. Comprende desde la explicación de los riesgos a los que están expuestos los activos de información, hasta la ejecución y seguimiento al cumplimiento de las normas y/o políticas informáticas. Las políticas de seguridad de la información también aplican para los servidores públicos en modalidad de teletrabajo.

POLÍTICAS DE IDENTIFICACIÓN Y PROTECCIÓN DE LA INFORMACIÓN Los activos de información dentro del alcance del Sistema de Gestión de Seguridad de la Información SGSI de la Personería Distrital de Cartagena de Indias, deben ser identificados, clasificados y definidos los responsables de cada uno de ellos. Busca asegurar que la información recibe el nivel de protección apropiado de acuerdo a la clasificación establecida.

POLÍTICA DE GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

En la Personería Distrital de Cartagena de Indias, la gestión de los riesgos fundamenta la toma de decisiones de seguridad de la información. Busca establecer la gestión del riesgo como eje principal de las actuaciones institucionales relacionadas con la seguridad de la información.

Servidores públicos y contratistas de la Personería Distrital de Cartagena de Indias, deben identificar y reportar condiciones que podrían indicar la existencia de riesgos de seguridad informática.

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

En la Personería Distrital de Cartagena de Indias, los eventos e incidentes de seguridad de la información son gestionados oportunamente con el fin de minimizar el impacto sobre la entidad. Busca establecer las líneas de actuación de los servidores públicos frente a la ocurrencia de situaciones que afecten la seguridad de la información.

POLÍTICA DE USO ADECUADO DE LOS RECURSOS DE LA PLATAFORMA DE TI

Toda la información de la Personería Distrital de Cartagena de Indias, así como los recursos para suprocesamiento, almacenamiento y transmisión deben ser empleados únicamente para propósitos laborales o de la entidad; evitando su abuso, derroche, uso ilegal o desaprovechamiento.

- Lineamientos generales de la gestión del riesgo de seguridad informática
- Requerimientos generales para el uso adecuado de la plataforma de TI.
- Se prohíbe el uso de los recursos de plataforma de T.I. de la Personería Distrital de Cartagena de Indias para la realización de cualquier actividad ilegal. 1.4.1.2. Para verificar el cumplimiento de las presentes políticas; la Personería Distrital de Cartagena de

Indias podrá monitorear y auditar las Plataforma de T.I.C. de la entidad que son facilitadas a servidores públicos y contratistas para el cumplimiento de sus deberes y funciones laborales.

- Los servidores públicos y contratistas deben abstenerse de crear, acceder, almacenar o transmitir material ilegal, pornográfico, que promueva la violación de los derechos humanos o que atente contra la integridad moral de las personas o de las instituciones.
- Está prohibida la realización de pruebas a los controles de seguridad de la información.
- No está permitido aprovechar las vulnerabilidades de seguridad de la plataforma de TI.

➢ Uso adecuado del correo electrónico

- No está permitido enviar correos masivos sin la autorización del personal directivo de la dependencia.
- El PU de Informática podrá establecer los límites en la cantidad de destinatarios y el tamaño de los mensajes de correo electrónico.
- No está autorizado el envío de correos electrónicos con contenido que atente contra la integridad y la dignidad de las personas, así como con el buen nombre de la entidad.
- Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico se retire de la Personería Distrital de Cartagena de Indias, su cuenta de correo será desactivada.
- Las cuentas de correo electrónico son propiedad de la Personería Distrital de Cartagena deIndias, son asignadas para la realización tareas propias de las funciones laborales.
- Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte dela Entidad.
- Cuando se detecte un correo fraudulento, con fines maliciosos o con contenido sospechosose debe informar esta situación al PU de Informática o a la mesa de ayuda del Centro de Servicios Informáticos.

➢ Uso adecuado de equipos de cómputo asignados

- No está permitida la instalación, ejecución y/o utilización de software diferente al preinstalado en los equipos de cómputo o al instalado por integrantes de los equipos de trabajo de informática.
  - Los parámetros de configuración del sistema operativo solo deben ser modificados por integrantes de los equipos de trabajo de informática.

➢ Uso adecuado de los servicios de red

- No deben almacenarse archivos personales en carpetas de la red y demás servicios de almacenamiento en internet suministrados por la Personería Distrital de Cartagena de Indias.
- No se permite el uso de servicios de descarga o intercambio de archivos que funcionan bajo el esquema P2P (person to person).
- La Personería Distrital de Cartagena de Indias, podrá controlar y limitar la navegación a ciertos sitios, recursos o servicios de internet con el fin de proteger la seguridad y la disponibilidad del servicio de internet.
- No está permitido deshabilitar o evadir los controles de navegación en internet.
- horarios laborales, está prohibido el uso del servicio de internet de la entidad para acceder a páginas de transmisión de películas, programas de televisión y eventos deportivos
- El acceso remoto a los equipos y dispositivos de la plataforma de T.I. solo está permitido para labores de soporte técnico autorizado.
  - El acceso remoto a equipos de cómputo debe contar con la aprobación del servidor público.
- Solo se permite el acceso remoto a estaciones de trabajo de la entidad si el servidor público responsable del equipo de cómputo lo aprueba.
- Solo está permitido el uso de servicios de almacenamiento de información suministrados por la entidad.
- La red de visitantes está dispuesta únicamente para las personas que visitan temporalmente la Personería Distrital de Cartagena de Indias.

➢ Uso de material protegido por derechos de autor

- Se prohíbe el almacenamiento de archivos multimedia (videos, música, imágenes o libros electrónicos) y cualquier otro tipo de contenido que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) en las carpetas de red y demás servicios de almacenamiento en internet suministrados por la entidad.
- Se prohíbe el almacenamiento, uso, instalación y/o ejecución de software que viole las leyesy regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) y/o licenciamiento en la plataforma tecnológica de la entidad.

POLÍTICA DE SEGURIDAD INFORMÁTICA PARA CONTRATACIÓN

La información de la Personería Distrital de Cartagena de Indias, debe ser protegida en el proceso de contratación. Busca proteger los procesos de contratación frente a situaciones que comprometan la disponibilidad, la integridad y la confidencialidad de la información de dichos procesos; resguardando así su legalidad y transparencia.

POLÍTICA DE SEGURIDAD FÍSICA DE LA INFORMACIÓN Y LOS EQUIPOS DE CÓMPUTO.

Se debe brindar seguridad física a la información de la entidad y a los recursos de la plataforma de T.I., de modo que se encuentren en condiciones ambientales adecuadas y a su vez, sean protegidosde situaciones como acceso no autorizado, robo, destrucción o desconexión.

Se pretende proteger la información, así como las tecnologías de información y la comunicación dela entidad frente a incidentes de seguridad causados por condiciones inadecuadas protección física,sean estas ambientales o que faciliten el acceso indebido a los activos de información.

➢ Seguridad en las instalaciones

- Fuera del horario laboral normal o cuando se alejen de sus estaciones de trabajo, los Servidores públicos y contratistas deben despejar sus pantallas, escritorios y áreas de trabajo, de talmanera que los datos, bien sean físicos (como documentos impresos y carpetas) o electrónicos (como memorias USB, Discos Duros Externos, CDs y DVDs), estén resguardados adecuadamente.
- Cuando un servidor público se percate de la presencia de personas sospechosas en las instalaciones de entidad, debe reportar dicha situación a la Dirección administrativa.
- No se deben prestar ni descuidar los elementos de identificación y acceso a las instalaciones de la Personería Distrital de Cartagena de Indias (tales como tarjetas de acceso, carnets, llaves y tokens).
- Cuando se imprima información clasificada o reservada, las impresiones deben ser retiradas inmediatamente.
- Siempre que sea posible, las impresiones deben ser protegidas por medio de una clave de seguridad.
- No está permitido fumar, ingerir alimentos o bebidas en las puestos de trabajo con equipos de cómputo.

➢ Seguridad de los equipos

- Los servidores públicos y contratistas de la Personería Distrital de Cartagena de Indias, son responsables de garantizar la debida protección de los equipos asignados (computadores de escritorio y dispositivos móviles) dentro y fuera de la entidad, lo que contempla su vigilancia, el debido cuidado en su transporte y el uso de cualquier otra medida de seguridad física necesaria.
- Los equipos suministrados por la Personería Distrital de Cartagena de Indias, como computadores de escritorio y dispositivos móviles (incluye computadores portátiles), no deben ser objeto de alteraciones en su hardware. Toda modificación a los equipos debe ser autorizada y realizada por personal de soporte técnico de los equipos.

- Se debe bloquear la sesión cuando el usuario se aleje del computador.
- La salida de los computadores (de escritorio o portátiles) de la entidad debe ser autorizada por la jefe de talento humano.
- Toda pérdida de equipos de cómputo o de alguno de sus componentes, debe ser informada inmediatamente al PU de informática.
- Los equipos de cómputo externos (no entregados por la Personería Distrital de Cartagena de Indias) no deben conectarse a la red de datos de la entidad, a menos que cumplan con los requisitos definidos por la oficina de sistemas. (Requisitos por definir).

POLÍTICA DE CONTROL DE ACCESO A PLATAFORMAS DE TECNOLOGÍA DE LA INFORMACIÓN.

La Personería Distrital de Cartagena de Indias, otorga el nivel de acceso necesario a la informacióny su plataforma de T.I. para el cabal cumplimiento de las funciones de los servidores públicos y contratistas. Se busca evitar y mitigar riesgos que comprometan la confidencialidad de la informacióny de las plataformas T.I.C. institucionales.

➢ Gestión de acceso a usuarios

- Los dueños de los sistemas de información deben verificar que los privilegios de acceso delos usuarios en las Plataformas de tecnología de la información se han otorgado de acuerdo con la necesidad laboral legítima.
- Los privilegios de acceso otorgados a los usuarios de las Plataformas de tecnología de la información deben ser autorizados por el superior inmediato. 1.7.1.3. Los privilegios de acceso otorgados a los usuarios de las Plataformas de Tecnología de Información deben ser revisados al menos anualmente por los jefes inmediatos de los usuarios.
- No están permitidas las cuentas de usuarios genéricas para el ingreso a la Plataforma de T.I.
- Todas las cuentas de usuario son personales e intransferibles.
- Servidores públicos y contratistas de la Personería Distrital de Cartagena de Indias, deben reportar a su jefe cuando tengan más derechos de acceso de los necesarios.

- excepción de las carpetas de red, los usuarios deben abstenerse de ingresar a los servidores de la plataforma tecnológica de la Personería Distrital de Cartagena de Indias, a menos que lo requieran en virtud de sus funciones laborales (como los Administradores de plataforma deT.I. de la entidad).
- En la eventualidad de requerirse el ingreso a un equipo o a alguna de las cuentas de los sistemas de información de la entidad asignadas a un servidor público ausente, el jefe directo respectivo será el único autorizado para solicitar el acceso.
- Los servidores públicos y contratistas son los responsables de todas las transacciones o acciones efectuadas con su cuenta de usuario.
- Ningún servidor público, contratista deberá acceder a la red o a los servicios de T.I.C. de la Personería Distrital de Cartagena de Indias, utilizando una cuenta de usuario diferente a la que lefue asignada.

➢ Manejo de contraseñas

- Los usuarios de las Plataformas de Tecnologías de la Información de la Personería Distrital de Cartagena de Indias, deben abstenerse de escribir las contraseñas en medios físicos o electrónicos.
- Las contraseñas de acceso a las Plataformas de Tecnologías de la Información son personales e intransferibles, cada usuario es responsable de su uso y de preservar su confidencialidad.
- El préstamo de contraseñas está prohibido bajo cualquier circunstancia, en caso de hacerlo el usuario de la información responsable de la cuenta asume las consecuencias generadas por dicha situación.

POLÍTICA DE OPERACIÓN DE PLATAFORMAS DE TECNOLOGÍA DE INFORMACIÓN

La Personería Distrital de Cartagena de Indias, aplica controles para el funcionamiento correcto y seguro de las Plataformas de tecnología de la información y la comunicación.

➢ Requisitos para la planeación y operación de las plataformas de TI.

- Los componentes y sistemas de la infraestructura de seguridad de la información, no debenser inhabilitados, desviados, apagados o desconectados sin la previa autorización del PU de informática.

➢ Protección contra software malicioso

- No está permitido el ingreso intencionado de software malicioso a los equipos y redes de laPersonería Distrital de Cartagena de Indias.
- La presencia identificada o sospechada de software malicioso debe ser reportada a la oficina de sistemas.

➢ Intercambio de información

- Personal de la mesa de ayuda del Centro de servicios Informáticos no está obligado a realizar procedimientos de recuperación de información borrada, debido a que no puede garantizarsela eficacia (el éxito) de la realización de estas actividades de recuperación.

POLÍTICAS DE CIFRADO DE LA INFORMACIÓN

Deben aplicarse mecanismos de cifrado cuando exista un alto riesgo de comprometer la confidencialidad de la información clasificada o reservada de la entidad. Busca establecer lineamientos tendientes a la protección de la confidencialidad de la información a través de mecanismos de cifrado.

- Servidores públicos y contratistas que sean responsables de llaves (o claves) de cifrado deben reportar al Equipo de Seguridad de la información, novedades acerca del manejo de dichas llaves (por ejemplo: cambio de dueños, cambio de custodia, pérdidas, acceso no autorizado).
- Cada vez que se utilice el cifrado, los servidores públicos y contratistas no deben borrar la única versión legible de los datos, a menos que hayan probado que el proceso de

descifrado puederestablecer una versión legible de los datos.

- Se deben utilizar mecanismos de cifrado cuando se requiera el almacenamiento de información reservada o clasificada en medios removibles (como memorias USB, discos duros externos, CD y DVD).
- Se deben utilizar mecanismos de cifrado cuando se requiera enviar información reservada oclasificada a través de redes externas (internet).

➢ POLÍTICA DE DISPOSITIVOS MÓVILES

El acceso a los datos y sistemas de información de la Personería Distrital de Cartagena de Indias, a través de dispositivos móviles debe ser realizado de forma regulada y controlada con el fin de evitar incidentes de seguridad de la información.

➢ Computadores portátiles

Los usuarios que tengan bajo su responsabilidad computadores portátiles de la Personería Distrital de Cartagena de Indias, son responsables de su protección dentro y fuera de las instalaciones de la entidad.

- Todo usuario al que se le asigne o facilite un computador portátil de la Personería Distritalde Cartagena de Indias, debe asegurarlo adecuadamente al puesto de trabajo en su gabinete con llave.
- Los usuarios de computadores portátiles de la Personería Distrital de Cartagena de Indias,deben emplear medidas de seguridad para su adecuado manejo fuera de las instalaciones de la entidad.

➢ Dispositivos móviles diferentes a computadores portátiles.

Esta sección hace referencia a dispositivos como teléfonos móviles inteligentes y tabletas.

- Los usuarios de dispositivos móviles entregados por la Personería Distrital de Cartagena de Indias, son responsables de su protección dentro y fuera de las instalaciones.
- Los usuarios de dispositivos móviles entregados por la Personería Distrital de Cartagena de Indias, deben abstenerse de modificar las configuraciones de seguridad de dichos dispositivos.

- Los usuarios de dispositivos móviles entregados por la Personería Distrital de Cartagena de Indias, deben reportar inmediatamente el robo o pérdida de dicho dispositivo al personal de los equipos de trabajo de informática.
- No está permitido el envío de información Clasificada o Reservada a través de servicios de mensajería instantánea no institucionales.
- La Personería Distrital de Cartagena de Indias, no está obligada a prestar soporte técnico a dispositivos móviles que sean de propiedad de los usuarios o cualquier otro que no sea propiedadde la entidad.
- Los usuarios que accedan a los servicios de la plataforma de T.I. (por ejemplo, al correo electrónico) a través de un dispositivo móvil propio, deben reportar inmediatamente el robo, cambio o pérdida de dicho dispositivo a la oficina de sistemas.

POLÍTICA DE CUMPLIMIENTO

La Personería Distrital de Cartagena de Indias, cumple la regulación y legislación vigente aplicable en materia de seguridad de la información. Busca identificar y asegurar el cumplimiento de los requisitos regulatorios y legales aplicables a la entidad en cuanto a la seguridad de la información.

➢ Cumplimiento legal y normativo

- Será sancionado con las acciones disciplinarias y legales correspondientes, al que utilice registros informáticos, software u otro medio para ocultar, alterar o distorsionar información requeridapara una actividad de la entidad, para el cumplimiento de una obligación respecto al Estado o para ocultar los estados contables o la situación de un proceso, área o persona física o jurídica.
- Toda la información de ciudadanos o servidores públicos y contratistas que incluya cédulas de identidad, datos de contacto o información financiera debe ser sólo accesible al personal de la entidad que necesite ese acceso en virtud de su trabajo.

POLÍTICAS PARA EL PERSONAL DE LOS EQUIPOS DE TRABAJO DE INFORMÁTICA

Estas Políticas aplican exclusivamente a personal de los equipos de Informática de la Personería Distrital de Cartagena de Indias ya sea interno o externo, en el ámbito del proceso de Planeación y Administración de las TI.

POLÍTICA DE GESTIÓN DEL RIESGO DE SEGURIDAD INFORMÁTICA

En la Personería Distrital de Cartagena de Indias, la gestión de los riesgos fundamenta la toma de decisiones de seguridad de la información. Busca establecer la gestión del riesgo como eje principal de las actuaciones institucionales relacionadas con la seguridad de la información.

➢ Lineamientos generales de la gestión del riesgo de seguridad informática

- Se deben identificar los riesgos a los que se encuentran expuestos los activos de informaciónde la entidad.
- Los criterios de evaluación y aceptación de riesgos de seguridad de la información deben estar alineados con los criterios y políticas de gestión del riesgo de la entidad.
- Los riesgos de seguridad de la información analizados deben ser objeto de tratamiento (mitigar, transferir, evitar, aceptar), dicho tratamiento debe ser coherente con los criterios de aceptación de riesgos.
- Los riesgos deben ser monitoreados después de su tratamiento para asegurar que siguen estando en niveles aceptables para la entidad.
- En los casos que se realice la estimación económica de los riesgos, se debe asegurar que el valor de la aplicación de medidas de mitigación sea inferior al costo de las consecuencias de la materialización de los riesgos.

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

En la Personería Distrital de Cartagena de Indias, los eventos e incidentes de seguridad de la información son gestionados oportunamente con el fin de minimizar el impacto sobre la entidad. Busca establecer las líneas de actuación de los servidores públicos frente a la ocurrencia de situaciones que afecten la seguridad de la información.

➢ Gestión de incidentes de seguridad de la información.

- Debe conformarse y mantenerse un equipo multidisciplinario para la respuesta y tratamientoa los incidentes de seguridad de la información.
- La atención de incidentes debe seguir el procedimiento descrito en el sistema de gestión dela calidad Gestión de Peticiones de Servicios e Incidentes.

POLÍTICA DE SEGURIDAD INFORMÁTICA ASOCIADA A CONTRATISTAS

La información de la Personería Distrital de Cartagena de Indias, debe ser protegida de los riesgos generados por el manejo o acceso de contratistas y proveedores. Busca mantener la seguridad de los activos de información accedidos por contratistas, evitando situaciones como: Abuso de privilegios de acceso. Fuga de información. Negación de responsabilidades de incidentes deseguridad por parte del contratista.

- Requisitos de seguridad de la información asociados a contratistas y terceros Solamente cuando se demuestre la necesidad de su uso y esté expresamente autorizado por el propietario del activos de información o sistema de información respectivo.
- Únicamente debe concederse acceso remoto a plataformas de TI a contratistas y proveedores cuando estos tengan una necesidad legítima que lo justifique.
- El tercero que ejerza funciones de administración y soporte de sistemas de información, debe garantizar que se generan registros automáticos (logs de auditoría) de dichas labores.

➢ SEGURIDAD FÍSICA DE LA INFORMACIÓN Y LOS EQUIPOS DE CÓMPUTO

Se debe brindar seguridad física a la información de la entidad y a los recursos de la plataforma de T.I., de modo que se encuentren en condiciones ambientales adecuadas y a su vez, sean protegidosde situaciones como acceso no autorizado, robo, destrucción o desconexión. Se busca proteger la información, así como las tecnologías de información y la comunicación de la entidad frente a incidentes de seguridad causados por condiciones inadecuadas protección física, sean estas ambientales o que faciliten el acceso indebido a los activos de información.

➢ Zonas restringidas de procesamiento

- Todo sistema, equipo, dispositivo, o medio crítico para la transmisión, procesamiento y almacenamiento de la información de la Personería Distrital de Cartagena de Indias, debe ser ubicado dentro de zonas restringidas de procesamiento. Si no se pudiera ubicar algún equipo dentro de estas zonas, dicho equipo debe ser objeto de controles complementarios de acceso físico.

- Sólo personal autorizado por el responsable de cada zona restringida de procesamiento puede ingresar a dicha zona.

➢ Seguridad física de los equipos

- Siempre que se reutilice un servidor, computador portátil o un computador de estación de trabajo, se requiere la realización previa de un formateo de la información almacenada en dichos equipos antes que sean entregados a los nuevos usuarios.
- Debe realizarse Borrado Seguro de los equipos de forma previa al proceso de disposición final (por ejemplo: venta, donación o destrucción).
- Los servidores deben estar ubicados de modo que se reduzcan los riesgos generados.

➢ CONTROL DE ACCESO A PLATAFORMAS DE TECNOLOGÍA DE LA INFORMACIÓN

La Personería Distrital de Cartagena de Indias, otorga el nivel de acceso a la información necesario para el cabal cumplimiento de las funciones. Busca evitar y mitigar riesgos que comprometan la confidencialidad de la información y de las plataformas T.I.C. institucionales.

➢ Proceso de control de acceso

- Todo proceso de control de acceso debe tener un responsable de su gestión. La gestión del proceso de control de acceso debe comprender las actividades de solicitud, aprobación,asignación, modificación y revocación del acceso.
- Cuando aplique, las medidas de control de acceso a las plataformas de tecnología de la información deben cumplir el Criterio de seguridad de la información.

➢ Gestión de acceso a usuarios

- Las cuentas de administración de las Plataformas de tecnología de la información sólo debenser usadas cuando sea necesario dicho privilegio.

➢ Manejo de contraseñas

- Los nombres de usuario y contraseñas se rigen por el Criterio de seguridad de la información de la Personería Distrital de Cartagena de Indias.
- No se permite el uso de contraseñas fijas. Todos los funcionarios sin excepción deben cambiar su password según lo establecido en el Criterio de seguridad de la Información.
- Las contraseñas de administración de las Plataforma de T.I.C. de tener un tiempo de caducidad, o en su defecto, deben ser cambiadas periódicamente. El periodo de vigencia de las contraseñas de administración de plataforma de T.I. se establece en el Criterio de Seguridad de la Información. (A desarrollar por la entidad).

➢ OPERACIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

La Personería Distrital de Cartagena de Indias, aplica controles para el funcionamiento correcto y seguro de las Plataformas de tecnología de la información y Telecomunicaciones. Busca proteger la operación de las plataformas de T.I.C. institucionales, garantizando la continuidad y la seguridad de los procesos institucionales.

➢ Requisitos para la planeación y operación de las plataformas de TI

- Toda intervención a las Plataformas de Tecnologías de la Información que impliquen modificaciones o cambios debe ser ejecutada de conformidad a lo establecido en el procedimiento de control de cambios.

- La realización de auditorías, verificaciones o pruebas de seguridad de la información no deben afectar la normal operación de las Plataformas de tecnología de la información.

➢ Respaldo de la información

- La información importante de la entidad alojada en los repositorios de red y los sistemas deinformación críticos deben ser respaldados a intervalos programados.
- Los respaldos de información deben ser probados regularmente, para verificar que la información si es recuperable ante un incidente.
- Los respaldos de información deben almacenarse además en un lugar externo a la Personería Distrital de Cartagena de Indias, evitando que ante la posibilidad de un desastre al interiorde la misma, se pierda por completo la información.

➢ Intercambio de información

- Las direcciones IP internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la entidad, deberán ser considerados y tratados como información clasificada.
- La creación de una conexión directa entre las Plataformas de tecnología de la información de la Personería Distrital de Cartagena de Indias y las organizaciones externas a través de Interneto cualquier otra red pública, debe estar autorizada por el PU de informatica.

➢ ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Los aplicativos y sistemas de información de la Personería Distrital de Cartagena de Indias, deben ser asegurados en sus fases de planeación, adquisición, desarrollo, implementación y operación. Se busca mitigar los riesgos de seguridad asociados a la existencia de seguridad en los aplicativos y sistemas de información de la entidad.

➢ Requerimientos de seguridad de los sistemas de información

- Durante la etapa de definición de requisitos para desarrollar, adquirir o modificar un aplicativo, se deben especificar claramente todos aquellos requisitos concernientes a la seguridad. Debe existir un registro que evidencie la documentación de tales requisitos.

➢ CRONOGRAMA

No	ACTIVIDAD	RESPONSABLE	FECHA IMPLEMENTACIÓN	VALORACIÓN
1	Agendamiento de entrevistas a lideres de proceso	Área de Sistemas	Enero 2024	10%
2	Entrevistas con los lideres de procesos.	Área de Sistemas	Febrero 2024	10%
3	Identificación de los riesgos.	Área de Sistemas	Febrero 2024	10%
4	Valoración de los riesgos.	Área de Sistemas	Febrero 2024	10%
5	Mapa de calor para ubicar los riesgos encontrados	Área de Sistemas	Febrero 2024	20%
6	Socializar el plan de tratamiento de riesgos de seguridad y privacidad de la información	Área de Sistemas	Marzo 2024	10%
7	Realizar seguimiento al plan de tratamiento de riesgos seguridad y privacidad de la información.	Área de Sistemas	Mayo , Agosto Y noviembre 2024	30%