PLAN DE SEGURIDAD

Y PRIVACIDAD DE LA INFORMACIÓN

2024

AGENCIA DE COOPERACIÓN E INVERSIÓN DE MEDELLÍN Y EL ÁREA METROPOLITANA
-ACI MEDELLÍN-

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CRISTINA ZAMBRANO RESTREPO
Representante Legal

NATALIA MARCELA MONÁ
Técnica de Sistemas de Información

2024

Contenido

1. INTRODUCCIÓN

La Agencia de Cooperación e Inversión de Medellín y el Área Metropolitana – ACI Medellín, ha reconocido la información como el activo más importante de la entidad, en este sentido se han incrementado los esfuerzos para fortalecer la protección de la misma, frente a factores de amenazas (externas) y debilidades (internas) que puedan poner en riesgo la misión y los objetivos institucionales, con la modernización de su infraestructura tecnológica la ACI Medellín busca promover una gestión segura y responsable de la información que se genera en el desarrollo de sus procesos para garantizar la integridad, confidencialidad y disponibilidad; sin embargo es importante resaltar la corresponsabilidad que tienen todos los funcionarios, contratistas y aprendices que interactúan con los recursos y sistemas de información.

2. OBJETIVOS

2.1 Objetivo general

Asegurar el uso adecuado de los sistemas de información y los recursos tecnológicos de la Agencia por parte de todos los funcionarios, contratistas y aprendices preservando, protegiendo y administrando de forma eficiente la información y los medios utilizados para su manipulación y procesamiento, con el fin de asegurar el cumplimiento de la integridad, confidencialidad y disponibilidad.

2.2 Objetivos específicos

- Informar y concientizar a todos los funcionarios, contratistas y aprendices de la Agencia sobre las políticas de seguridad y privacidad de la información, minimizando las amenazas que puedan afectar el mayor activo de la entidad.
- Verificar la aplicación de las políticas de seguridad en los equipos de cómputo, usuarios finales y los sistemas de información.

3. ALCANCE

El Plan de Seguridad y Privacidad de la Información define las políticas, conceptos y campos de aplicación para todos los procesos institucionales, con el objetivo de cumplir con los lineamientos de las TI en el proceso de una gestión responsable frente a la información.

4. DEFINICIONES

Confidencialidad: garantizar que la información sea accesible sólo por las personas autorizadas.
Integridad: conservar la exactitud y totalidad de la información y los métodos de procesamiento.
Disponibilidad: permitir acceso a los usuarios que estén autorizados a la información y a los recursos informáticos toda vez que lo requieran.
Adicionalmente, deberán considerarse los conceptos de:
Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto la entidad.
Confiabilidad de la información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
MSPI: Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones – MinTIC.
Partes Interesadas: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Para los efectos de una correcta interpretación del presente plan, se describen las siguientes definiciones:

✓ Spoofing: uso de técnicas de suplantación que a través de las cuales un atacante, con fines maliciosos o de investigación se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

✓ Phishing: técnica con base a la ingeniería social que trata de adquirir información de forma fraudulenta engañando e incitando al usuario que entregue información confidencial a través de páginas falsas, correos o incluso llamadas telefónicas.

✓ Routers: dispositivo de red de capa 3 diseñado para administrar el tráfico entre diferentes redes dependiendo de las reglas establecidas.

✓ Switches: dispositivo de red de capa 2 que se encarga de establecer la conexión física entre los diferentes equipos de red basado en sus direcciones físicas.

✓ Access Point: dispositivo de red que permite conexiones inalámbricas de diferentes tecnologías como son 802.11a, 802.11b, 802.11g entre otros.

✓ RDSI: sus siglas traducen Red Digital de servicios Integrados y es una tecnología de conectividad WAN digital y punto a punto que consta de canales BRI (de 64kbps cada uno) para el transporte de datos más un canal D (de 16 kbps) para fines de señalización.

✓ Keylogger: software que se puede utilizar para fines maliciosos el cual guarda un log local con todas las teclas que el usuario digite en el equipo donde está instalado.

✓ Port Scanner: software que realiza un escaneo de puertos contra una dirección ip específica. Revela muchas de las vulnerabilidades de los sistemas a nivel perimetral y de aplicación.

✓ DoS: traduce ataques de denegación de servicio y es una técnica que busca que un recurso sea inaccesible para usuarios legítimos.

✓ SMTP: protocolo simple de transferencia de correo el cual está basado en texto utilizado para el intercambio de mensajes de correo electrónico entre dispositivos. Es el protocolo responsable de enviar los correos.

✓ Programas Peer-to-Peer: programas que utilizan a todos los otros usuarios de la red de internet para compartir información, por lo cual todos son clientes y servidores al tiempo. Entre los más destacados actualmente se encuentran, limeWare, Emule, Azure, BitTorrents y Kazza.

✓ Proxys Piratas: pueden ser páginas o software que enmascaran las URL (páginas de navegación) reales a las que el usuario está accediendo con el objetivo de tratar de violar los controles que se tienen de manera que no descubra a donde estaban accediendo realmente.

✓ Incidente de seguridad: evento que viole, o que intente violar la seguridad informática, se considera violación de la seguridad informática, el hecho que un individuo intente, ejecute o encubra acciones y tenga acceso a información no autorizada para su uso o modificación.

✓ Política de seguridad: es una declaración formal de las reglas que deben seguir las personas con acceso a los activos de tecnología e información, dentro de la ACI.

✓ Procedimientos: constituyen la descripción detallada de la manera como se implementa una política.

✓ Virus informático: programa ejecutable o segmento de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos (información) y reducción del desempeño de un equipo de cómputo.

✓ GPO: es un conjunto de políticas del sistema, desplegadas mediante el directorio activo de la ACI y se aplican apenas el usuario inicia sección en alguno de los equipos de cómputo de la agencia.

✓ VPN: una VPN (Virtual Private Network) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

✓ IaaS: La infraestructura como servicio (IaaS) es un método para ofrecer funcionalidades de computación, almacenamiento, redes y de otros tipos a través de Internet en nube privada.

✓ Ingeniería social: es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.

✓ Modalidad de teletrabajo Suplementario: trabajadores con contrato laboral que alternan sus tareas en distintos días de la semana entre la empresa y un lugar fuera de ella usando las TIC para dar cumplimiento. Se entiende que teletrabajan al menos dos días a la semana.

✓ Modalidad de teletrabajo Móvil: trabajadores que utilizan dispositivos móviles para ejecutar sus tareas. Su actividad laboral les permite ausentarse con frecuencia de la oficina. No tienen un lugar definido para ejecutar sus tareas.

✓ Modalidad de teletrabajo autónomo: trabajadores independientes o empleados que se valen de las TIC para el desarrollo de sus tareas, ejecutándolas desde cualquier lugar elegido por ellos.

5. ROLES Y RESPONSABILIDADES

- **Comité Directivo:** aprueban los lineamientos conceptuales y metodológicos definidos en la GI-SIG-01 guía de administración de riesgos, es responsable de fortalecer, incentivar y hacer cumplir las políticas allí definidas.
- **Subproceso del Sistema Integrado de Gestión:** es el encargado de generar la metodología para la administración de riesgo; coordina, lidera, asesora y capacita en su objeto funcional.

- **Integrantes de los procesos institucionales:** identifican, analizan y valoran los riesgos del proceso o subproceso por lo menos una vez al año, si bien están apoyados por el Profesional Senior en Calidad, son los responsables de garantizar que en el proceso se definan los riesgos de la información que le competen, se establezcan los controles y se adelanten las actividades para mitigarlos.
- **Contratistas**: ejecutar en sus funciones los controles y acciones definidas en los lineamientos de la administración del riesgo, también aportan a la identificación de posibles amenazas que puedan afectar la información institucional.
- **Control Interno**: su responsabilidad es verificar y evaluar la elaboración, la visibilizarían, el seguimiento y el control del mapa de riesgos, conforme a la GI-SIG-01 guía de administración de riesgo.

Auxiliar administrativo sistemas de información: identificar vulnerabilidades en los sistemas de información e infraestructura informática, hacer ajustes necesarios para corregir y disminuir los riesgos informáticos. Auditar el cumplimiento de las políticas y notificar a través de informes a la dirección de relaciones administrativas los casos de no cumplimiento. Elaborar planes, campañas de divulgación de las políticas a todos los usuarios y otras estrategias de tipo preventivas. Proveer los recursos necesarios para la correcta operación y cumplimiento de estas políticas. Sensibilizar al comité directivo de la Agencia de la importancia de estas políticas de seguridad para el éxito de estas.

6. DIAGNÓSTICO

En el año 2015 la ACI Medellín adopta dentro de su lista de manuales el MN-GSI-01 Manual de Políticas de Seguridad y Privacidad aprobado y con el visto bueno desde el comité directivo, desde ese momento se ha venido actualizando y ajustando acorde a las necesidades y cambios que ha tenido la entidad en sus sistemas de información, su aplicación y cumplimiento se despliega a todos los funcionarios, contratistas y terceros que interactúen con los sistemas de información e infraestructura tecnológica de propiedad de la Agencia.

Desde el subproceso de Sistema Integrado de Gestión se estipuló la GI-SIG-01 Guía de Administración de Riesgos, la cual tiene como objetivo: Establecer disposiciones y criterios institucionales que orienten a la ACI Medellín en la correcta identificación, análisis, valoración y administración de los riesgos, con el fin de reducir la probabilidad de ocurrencia y el grado de impacto de aquellos riesgos que pueden afectar el logro de los objetivos institucionales en el marco de los procesos. Desde la administración del riesgo se maneja los Mapas de Riesgos en los cuales se identifican los riesgos desde cada proceso aplicados a la información institucional y con las políticas de seguridad.

7. DESCRIPCIÓN DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

7.1 Acceso a la información

- ✓ La información es un recurso que, como el resto de los activos, tiene valor para la Agencia siendo este el activo más importante, su manejo influye en el objetivo de alcanzar la misión institucional y está expuesta a problemas de seguridad, por consiguiente, debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos y contribuyendo de esta manera, a una mejor gestión de la información.
- ✓ Todos los funcionarios que laboran para la ACI Medellín independiente de su modalidad de contratación o método de conexión deben tener acceso sólo a la información necesaria para el desarrollo de sus funciones. Es responsabilidad de los directores de cada proceso solicitar el acceso de acuerdo con el trabajo realizado por el personal a su cargo.
- ✓ El uso de los sistemas de información de la entidad, servicios de red y correo deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la entidad.
- ✓ Toda la información contenida, procesada o generada en los equipos de cómputo, bases de datos o sistemas de información de ACI Medellín es de su propiedad incluso si se realizó en dispositivos ajenos a la entidad.

7.2 Seguridad de la información

- ✓ Los funcionarios que laboran en la ACI Medellín son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la entidad y por la normativa que la proteja, tendiente a evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma. Entre esta información tenemos la siguiente: hojas de Excel, documentos tipo Word, documentos tipo PowerPoint, correo electrónico, PDF, o algún otro sistema de información que use la entidad.
- ✓ Todos los funcionarios que utilicen los recursos informáticos tienen la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como pública clasificada, pública reservada o pública.
- ✓ No se deben dejar visibles las contraseñas de correo, red y archivos, ya que pueden ser utilizadas por otras personas alterando o dañando su información, tampoco se deben compartir sus contraseñas ya que pueden ser utilizadas con otros objetivos.
- ✓ No debe permitir que personal externo consulte o gestione su información.
- ✓ Al desplazarse de su puesto de trabajo, bloquee la sesión en el equipo, esto evita posibles ingresos no autorizados a su información.

7.3 Seguridad de los sistemas de información

- ✓ La plataforma Office 365, herramientas colaborativas, CRM institucional, unidades de red, software contable, software gestión documental, son utilidades asociadas de la entidad que debe ser usado únicamente para el ejercicio de las funciones y actividades de competencia de cada usuario.
- ✓ El uso de la red Internet debe ser solo para fines laborales, no está permitido el ingreso a páginas del siguiente tipo: pornografía, radio y tv, juegos, armas, sitios maliciosos, software free, entre otros.
- ✓ Contraseñas
  La contraseña debe de cumplir con una longitud mínima de 8 caracteres, y al menos con tres tipos entre los siguientes caracteres:
  - Letras Mayúsculas
  - Letras Minúsculas
  - Números en sustitución de letras (1 por I, 0 por o, 3 por la E, etcétera)
  - Caracteres especiales no alfanuméricos, como signos de puntuación
  - Cada 42 días el sistema le exige que cambie su contraseña de red.

7.4 Seguridad en recursos informáticos

Todos los recursos informáticos deben cumplir con lo siguiente:

- ✓ Administración de usuarios: establece como deben ser utilizadas las claves de ingreso a los recursos informáticos y da parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiarlas, entre otras. Lo anterior se encuentra configurado en los controladores del dominio de la ACI con GPO (Group Policy Object).

- ✓ Rol de usuario: los sistemas de información, bases de datos y aplicativos deberán contar con roles predefinidos, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol desarrolle la administración de usuarios.

- ✓ Control de acceso: el ingreso a todos los sistemas de información de la entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario. Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los usuarios de la ACI son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

- ✓ Activos de información: Toda la información que sea sensible, crítica o valiosa debe tener controles de acceso para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.

7.5 Seguridad en comunicaciones

- ✓ 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 confidencial.

- ✓ Todas las conexiones a redes externas o que accedan a la red interna de la entidad deben pasar a través de los dispositivos sistemas de registro de directorio activo de la entidad, que incluyen servicios de inscripción y verificación de datos, detección de ataques e intentos de intrusión, administración de permisos de circulación y autenticación de usuarios. Administrado desde el firewall de seguridad perimetral Fortigate 40E.

7.6 Software utilizado

- ✓ Todo software que utilice la Agencia será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la entidad o reglamentos internos.

- ✓ Todo el software de manejo de datos que utilice la Agencia dentro de su infraestructura informática deberá contar con las técnicas más avanzadas para garantizar la integridad de los datos.

- ✓ Debe existir una cultura informática al interior de la entidad que garantice el conocimiento por parte de los usuarios, contratistas y practicantes de las implicaciones que tiene el instalar software ilegal en los computadores de la Agencia.

- ✓ La instalación de software en los equipos de cómputo estará controlada mediante configuración especial en dichos computadores y administrada desde los servidores, la cual solicitará usuario y contraseña del administrador al momento de realizar una instalación, esto asegura que ningún programa o software podrá ser instalado en los computadores; a su vez el personal de sistemas deberá intervenir en dicha instalación ya que son los autorizados para manejar las contraseñas de administrador.

7.7 Actualización de hardware

Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del personal de sistemas.

La reparación técnica de los equipos, que implique la apertura de estos, únicamente puede ser realizada o autorizada por el personal de sistemas y se documentará cuando no exista garantía vigente de las partes a reemplazar.

Los computadores e impresoras no deben reubicarse sin la aprobación previa del personal de sistemas.

7.8 Almacenamiento y respaldo

- ✓ La información que es soportada por la infraestructura de tecnología informática de la ACI Medellín deberá ser almacenada y respaldada de acuerdo con las buenas prácticas de TI de tal forma que se garantice su disponibilidad.

- ✓ Cada usuario tiene asignadas unidades de red de acuerdo con el proceso al que pertenece, toda información que sea generada por sus funciones en la Agencia debe ser almacenada en dichas unidades y no en otro lugar, ya que estos recursos son a los que se les aplica las copias de seguridad.

- ✓ Los usuarios son responsables de la información en los computadores, siguiendo las indicaciones técnicas dictadas por el personal de sistemas.

- ✓ El personal de sistemas define la estrategia a seguir para el respaldo de la información.

- ✓ No instalar (sincronizar) servicios de almacenamiento en la nube diferentes al OneDrive, y mucho menos manejar información institucional en estos sistemas de almacenamiento.

- ✓ Solo se permitirá almacenar información en la nube mediante la herramienta institucional de Office 365 - OneDrive.

- ✓ La información de tipo audio, video, imágenes y archivos personales, no están permitidos en los recursos de almacenamiento dispuestos por la ACI.

- ✓ La información de tipo audio, video, imágenes generadas por la labor en la ACI debe ser almacenada en la unidad de red de Fotos_Aci.

7.8.1 Esquema de la estrategia de respaldo de la información (generacional)

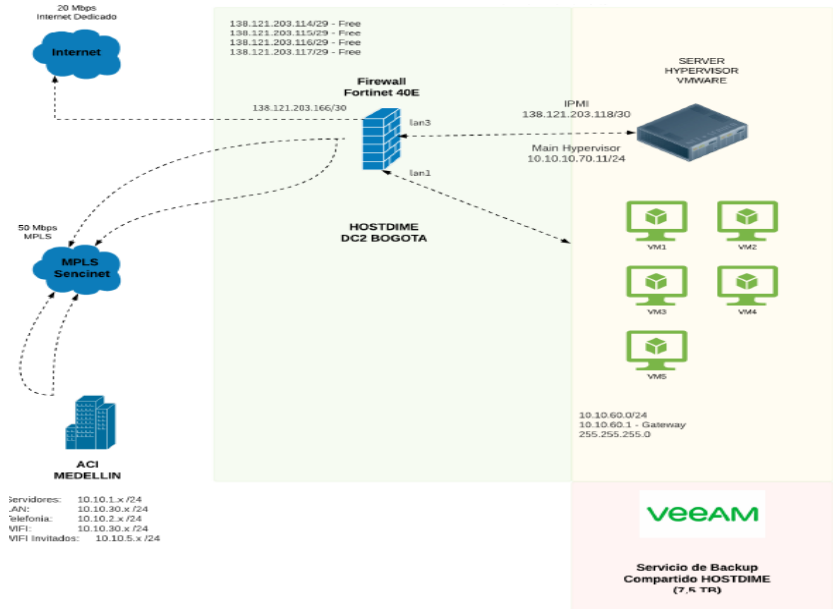

Figura 1. Esquema de conexión. Hostdime

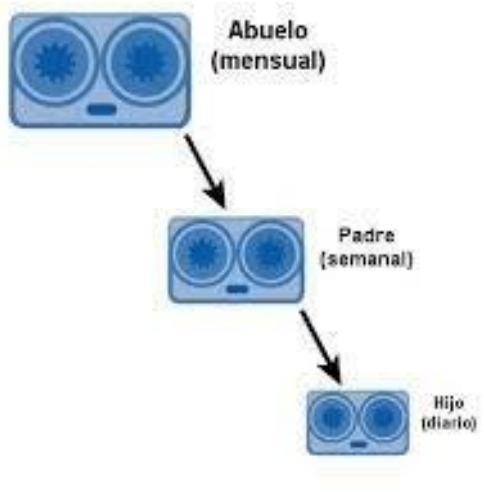

Figura 2. Esquema de copias

7.8.2 Descripción técnica de respaldo de información

Una copia de seguridad generacional es uno de los métodos más simples y eficaces de crear y conservar copias de seguridad de los datos. Si se realiza correctamente, combina la facilidad de uso y la protección de datos.

El esquema de copia de seguridad generacional más común es el método de tres generaciones o "abuelo-padre-hijo", en su forma más básica, implica realizar una copia completa de los datos que deben guardarse en un medio extraíble como, por ejemplo, cintas o discos duros, este es el abuelo, en el siguiente período programado de copia de seguridad, por ejemplo, al día siguiente, se realiza otra copia completa de los datos que, por supuesto, incluye los cambios realizados en los datos durante ese período, es el padre, en la siguiente copia de seguridad programada, se produce la tercera copia, o hijo.

La cuarta copia de seguridad se realiza grabando encima (o sustituyendo, según el medio) la copia "abuelo", la nueva copia se convierte en "hijo", el hijo anterior pasa a ser el nuevo "padre", y el padre asciende a "abuelo". Esto continúa de manera rotatoria de manera que siempre hay tres copias de seguridad, cada una de ellas de un momento diferente.

Nota: para cada año se tendrá una cinta nueva disponible para la copia del mes doce, dicha cinta no tendrá cambios en el tiempo y se conservará en el archivo de la Agencia siendo está el soporte de la información cada año.

- **Copia de seguridad completa:** almacena todos los datos seleccionados para la copia de seguridad y forma la base para una copia de seguridad incremental.

- **Copia de seguridad incremental:** almacena todos los cambios desde la copia de seguridad completa. Necesita tener acceso a otras copias de seguridad del mismo archivo para recuperar los datos con una copia de seguridad incremental.

7.8.3 Programación de copias de seguridad

La entidad cuenta con una infraestructura tecnológica a través de nube privada y se tienen programadas las copias de seguridad de la siguiente manera:

Mensual (Abuelo): corresponde a los datos que se generan durante el mes y el medio de almacenamiento de dicha información es en un cartucho de cinta magnética la cual esta custodiada con un proveedor experto en custodia de archivos, es una copia completa y se realiza los días 30 de cada mes.

Semanal (Padre): corresponde a todo el dato generado en la semana, el medio de almacenamiento es en disco, los cuales están ubicados en los servidores de la Agencia, es una copia completa de archivos. Se realiza el sábado de cada semana.

Diaria (Hijo): corresponde a todos los datos generados en el día, el medio de almacenamiento es en disco, los cuales están ubicados en los servidores de la Agencia, es una copia incremental de los datos. Se realiza de lunes a viernes.

Nota: todas estas copias se realizan mediante la aplicación VEEAM BACKUP.

7.9 Soporte técnico

Todo requerimiento debe ser registrado mediante el portal de soporte (Soporte Remoto Zoho), ubicado como acceso directo en el escritorio de cada usuario. Allí se debe ingresar la información clara del inconveniente a reportar, se debe escoger el tipo de soporte según sea su caso, requerimiento o solicitud.

Nota: el portal de soporte será el único medio para brindar el servicio de soporte mediante el ticket generado por la herramienta de CRM institucional.

7.10 Protección contra virus

El virus por computador puede definirse como un: programa con capacidad de reproducir un error (infección) e insertarlo en las áreas de datos, de programas del mismo sistema y alterar su normal funcionamiento. Estos atacan destruyendo la integridad de la información contenida en los medios de almacenamiento magnético llegando incluso a dañar partes físicas de la máquina.

Aunque existe software antivirus, lo primordial es prevenir el contagio mediante la adopción de una política de sano procesamiento que el usuario debe seguir:

- ✓ Hacer un escaneo con el servicio de antivirus institucional a todo documento, imagen, video, medio magnético, descargas online, adjuntos de correo electrónico; previniendo el ingreso de virus informática y demás riesgos que esto conlleva.
- ✓ Utilizar únicamente software autorizado e instalado por el auxiliar administrativo de sistemas e informática.

Desde la consola de administración del antivirus se tienen programados unas actualizaciones y escaneos en segundo plano los viernes después de las 12 pm, generando un reporte mensual de lo encontrado.

7.11 Hardware

- ✓ El equipo de cómputo será asignado de acuerdo con el puesto o función laboral en su proceso.
- ✓ Cada equipo está preparado con el hardware y software básico necesario para su funcionamiento, el usuario no deberá alterar el contenido físico y lógico del mismo incluyendo sus periféricos.
- ✓ En caso de presentar una falla física o lógica se deberá notificar al auxiliar administrativo de sistemas de información.

- ✓ En ningún caso el usuario intentara reparar el equipo o diagnosticarlo, únicamente informar de la posible falla.
- ✓ El usuario será el único responsable del equipo de cómputo.
- ✓ Solo se utilizará el equipo para funciones de interés de la ACI y de ninguna manera para asuntos personales.
- ✓ Cada equipo contiene el software de acuerdo con las necesidades de las funciones a desempeñar.
- ✓ Por ningún motivo el usuario instalará software de promoción y entretenimiento.
- ✓ La adquisición o desarrollo de software será responsabilidad del auxiliar administrativo de sistemas de información.

7.12 Pautas para el uso autorizado del correo electrónico

El servicio de correo electrónico de la Agencia está habilitado exclusivamente para apoyar la gestión misional y administrativa de la entidad. Esto significa que el funcionario o persona autorizada utiliza este servicio para los propósitos de misión y razón de ser de la ACI y la comunicación con entidades, empresas, proveedores, clientes y contratistas.

Las siguientes son recomendaciones específicas con respecto al uso autorizado del buzón de correo electrónico que se asigna a un funcionario o persona autorizada dentro de la ACI:

Usos autorizados

- ✓ Los buzones de correo electrónico tienen un tamaño de 100GB para todos los funcionarios, este servicio se encuentra disponible en la nube mediante Office 365 y es responsabilidad del usuario velar por la seguridad del ingreso a la plataforma fuera de las instalaciones de la Agencia.
- ✓ Desconfíe de aquellos e-mails en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial, etc.
- ✓ Se permite la suscripción a listas de distribución y otras formas de los servicios de la suscripción del correo electrónico relacionados con la función del trabajo.
- ✓ El uso del correo electrónico como recurso institucional asignado debe manejarse con conducta ética y responsable, acatando el mandato legal vigente relacionado con el uso de recursos tecnológicos o cualquier otra regulación interna expedida en este sentido por la entidad.

Uso prohibido

Los funcionarios o personas autorizadas de la Agencia no utilizaran el servicio de correo electrónico para crear, ver, guardar, recibir, o enviar material de los siguientes casos:

- ✓ No utilizar la cuenta de correo electrónico institucional, en redes sociales como Facebook, Instagram u otro tipo de red que envié notificaciones o información al buzón que no tiene nada que ver con la Agencia.

- ✓ Crear o intercambiar mensajes ofensivos u obscenos de cualquier clase, incluyendo material pornográfico.
- ✓ Enviar correo electrónico que contenga amenazas o mensajes violentos.
- ✓ Intercambiar mensajes con información confidencial con personas externas o ajenas a la entidad.
- ✓ Creación, reenvió o intercambio de mensajes SPAM (correo no solicitado), cadenas de cartas, solicitudes o publicidad.
- ✓ Crear, almacenar o intercambiar mensajes que contengan material protegido bajo las leyes de derechos de autor, sin el consentimiento de sus autores.
- ✓ Divulgar mensajes con datos o información institucional no autorizada.
- ✓ Divulgar sus contraseñas de correo.
- ✓ Alterar el contenido del mensaje de otro usuario sin su consentimiento.
- ✓ Utilizar como propia la cuenta de correo de otro funcionario sin su permiso.
- ✓ Inscribir la cuenta de correo en listas no relacionadas con la gestión de la entidad.
- ✓ Borrar mensajes cuyo contenido es relevante o importante, dentro de las funciones asignadas como funcionario o para la entidad.
- ✓ Enviar mensajes con archivos anexos extensos, que puedan afectar el desempeño del servicio y de la red local.

Privacidad

Los funcionarios, usuarios o personas autorizadas no deben mantener expectativa de privacidad, mientras estén usando el correo electrónico de la ACI; Además, la información que transite temporalmente o se almacene de manera permanente en los recursos informáticos de la Agencia será monitoreada, la ACI Medellín mantendrá el derecho de monitorear y revisar el contenido enviado o recibido por los funcionarios a través del servicio de correo electrónico, cuando sea necesario, tales comunicaciones no deben ser consideradas como privadas o seguras.

8. VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD

Las siguientes actividades son consideradas como violaciones a las políticas de seguridad:

- ✓ Enviar correo electrónico no solicitado o Spam.
- ✓ Envío de correo con contenidos pornográficos.
- ✓ Instalación o ejecución de software no autorizado.
- ✓ Utilización del internet indebidamente, esto incluye, navegación a páginas con contenidos pornográficos, sitios de música en línea, juegos en línea, sistemas de mensajería instantánea (no autorizados), casinos, proxys piratas, programas de carga de archivos, o cualquier otro sitio con fines diferentes a los laborales.
- ✓ Traslado o instalación de nuevos equipos a la red sin la autorización ni el procedimiento establecido por el subproceso de recursos tecnológicos.
- ✓ Dañar física o lógicamente los equipos o la infraestructura informática.
- ✓ Instalar dispositivos o tarjetas de acceso remoto, módems, RDSI, Routers o cualquier otro dispositivo de comunicaciones en los clientes de la red.

- ✓ Utilizar cualquiera de los recursos informáticos de la Agencia para fines diferentes a las funciones contractuales, ya sea funcionario o contratista.
- ✓ Utilizar cualquier tipo de software para fines malicioso o intrusos tales como sniffers, port scanner, keyloggers, entre otros.
- ✓ Utilizar cualquier técnica de hacking hacia cualquiera de los recursos tecnológicos de la Agencia entre los que se incluye, ataques DoS, phising, spoofing y broadcast storm.
- ✓ Violación o cambio de contraseñas.
- ✓ Usar cuentas de equipos sin autorización.
- ✓ Conseguir acceso no autorizado a cualquier equipo o información.
- ✓ Conseguir acceso no autorizado a los recursos compartidos, almacenados en los equipos y servidores de la infraestructura informática.
- ✓ Acceso sin autorización a equipos de red tales como servidores, Routers, Switches, Access Point, Firewalls, u otros appliance de red de la Agencia o que estén en sus instalaciones.
- ✓ Ejecución intencionada de scripts que comprometan la seguridad y buena utilización de los recursos.
- ✓ Ejecutar una base de datos con el propósito de recolectar datos contenidos en ella.
- ✓ Acceso no autorizado a sistemas críticos y delicados como ARIES sistema contable, Docuware sistema de gestión documental y bases de datos, CRM institucional, unidades de red no autorizadas.
- ✓ Realizar o modificar transacciones indebidas en cualquier sistema financiero implementado en la Agencia como lo son algunos de los módulos de ARIES.
- ✓ Ejecución de comandos SNMP a servidores de correo.
- ✓ Utilizar cualquiera de los recursos informáticos de la Agencia para fines lucrativos diferentes a los contratos.
- ✓ Las violaciones de las políticas de seguridad y privacidad por parte de funcionarios y contratistas o usuarios de los recursos tecnológicos darán lugar a la respectiva investigación de carácter disciplinario, penal, civil y fiscal a que haya lugar.

9. PROPIEDAD INTELECTUAL

La ACI Medellín es propietaria y podrá tener acceso en el momento que sea necesario a cualquier información alojada en los equipos que son de su propiedad o a los que suministra licencias y/o conectividad, incluye equipos de cómputo, servidores, almacenamiento, recursos compartidos entre otros, así mismo podrá tener acceso a cualquier información generada y transmitida por la red.

Todos los computadores y servidores de la ACI Medellín deberán pertenecer al dominio denominado ACIMEDELLIN.LOC y sujetarse a las políticas de seguridad que estén establecidas actualmente, por lo tanto, cualquier software que se esté instalando en las maquinas deberá tener su respectiva licencia y previa autorización por parte del auxiliar administrativo sistemas de información para su correcto funcionamiento.

Se debe tener en cuenta que cualquier acción dentro del dominio se registra con el nombre de usuario individual, por lo cual los usuarios y claves del dominio son personales e intransferibles y cada uno es responsable de la utilización y del buen uso que les dé a los elementos informáticos, tales como uso del internet, correo, almacenamiento y transferencia de archivos, carpetas compartidas, y utilización de las aplicaciones.

La Agencia de Cooperación e Inversión de Medellín y el Área Metropolitana ACI tienen la intención de hacer cumplir esta política, pero se reserva el derecho de cambiarla en cualquier momento si las circunstancias así lo ameritan.

10. TRATAMIENTO DE DATOS PERSONALES

La ACI Medellín dentro de sus manuales adopta el MN-DES-01 Manual de Tratamiento de Datos en atención a lo determinado por la Ley 1581 de 2012, el cual consiste en desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Este manual, es de obligatorio cumplimiento por parte de todos los funcionarios, contratistas, y terceros que obren en nombre de la ACI Medellín en ejercicio de sus funciones y de obligaciones contractuales. Consulte el manual aquí.

11. ACTIVIDADES VIGENCIA 2024

El Subproceso de Gestión de Sistemas de Información proyecta las actividades en el plan operativo anual de acuerdo con los procedimientos definidos, en el que se vinculan las partes interesadas además de los sistemas de información y la infraestructura tecnológica, teniendo en cuenta la normatividad del estado realizando un adecuado uso y tratamiento de la información gestionada por la Agencia en términos de confidencialidad, integridad y disponibilidad.

- ✓ Socializar a los funcionarios nuevos y contratista por medio de la inducción las políticas de seguridad y privacidad de la información y el teletrabajo haciendo énfasis en su importancia tanto para el usuario como para la entidad.
- ✓ Dar a conocer las políticas de seguridad y privacidad de la información a toda la entidad mediante reuniones por proceso, boletines y flash informativos que refuercen y apoyen el apoderamiento de las políticas de seguridad y privacidad de la información en los funcionarios.
- ✓ Identificar proveedores críticos que interactúen con la información de la entidad, con el objetivo de tener un inventario de los terceros que proporcionan o soportan

servicios necesarios para el funcionamiento de la Agencia y puedan representar riesgos frente a la información institucional.

12. DEFINICION DE SEGURIDAD Y TELETRABAJO

La seguridad se concibe como un conjunto de medidas que son implementadas para disminuir el riesgo, aumentar la protección y garantizar el bienestar de los objetos o individuos.

Esta se tiene presente en los diferentes ámbitos de la vida teniendo en común los siguientes aspectos:

•Las condiciones para asegurar las actividades que se desarrollan.
•Los riesgos que se presentan desarrollando dicha actividad (internos y externos).
•Las acciones a tomar para mitigar los riesgos.
•Tomar medidas preventivas para evitar los riesgos de seguridad.

Con la evolución de las TIC se hizo necesario establecer medidas de protección de la infraestructura y de la información, a lo cual se denomina seguridad informática. Este concepto ha ido evolucionando al ritmo de la tecnología; inicialmente se consideraba solo la protección física de los equipos de telecomunicaciones con el objeto de evitar daños o robos, posteriormente se consideró la protección de las redes limitando su acceso, y hoy en día se considera también la protección de un activo valioso como es la información.

En la modalidad de teletrabajo el subproceso de Gestión de Sistemas de Información debe velar por garantizar la seguridad de la información, tanto de los equipos como de los teletrabajadores. Estos últimos trasladan numerosos datos y contenidos a dispositivos electrónicos con nuevas ubicaciones físicas generando nuevos riesgos que se deben mitigar estableciendo protocolos adecuados. Tales políticas de seguridad se establecen como planes de acción encargados de afrontar, mitigar y prevenir los riesgos originados con la implementación del teletrabajo.

Con relación a la información, dado que esta se considera como el recurso intangible de mayor importancia, es necesario mantener y garantizar con el fin de prevenir cualquier anomalía los servicios de antivirus, respaldo o backup, acceso seguro a través de VPN (Virtual Private Network - Red Privada Virtual) y acceso restringido a aplicaciones. Por otro lado, la definición de las políticas de seguridad de la ACI Medellín debe garantizar:

• Confidencialidad: asegurar el acceso a la información únicamente por las personas autorizadas, que son los teletrabajadores.
• Integridad: mantener los datos libres de modificaciones no autorizadas.
• Disponibilidad: garantizar que la información esté en disposición para los teletrabajadores en cualquier momento, de tal forma que puedan desarrollar sus

actividades.
• Autenticación: identificar al usuario generador de la información.

De igual forma como se debe propender por reducir las amenazas relacionadas con los recursos intangibles, también se deben establecer los procedimientos relacionados con la protección de los recursos tangibles a través de un análisis de riesgos ocasionados por la implementación de teletrabajo, como lo son los procesos de manejo de equipos, pólizas de seguros, mantenimiento de equipos, entre otros.

Se establecen patrones de seguridad adecuados con la implementación del teletrabajo contemplando objetivamente tanto las necesidades de la entidad como las del teletrabajador, así como se consideren los posibles riesgos exógenos y endógenos que realmente pueden afectar el desarrollo de las labores del teletrabajador.

13.POLÍTICAS.

13.1 Políticas de dispositivos móviles.

✓ La ACI Medellín establece las condiciones para el uso seguro de los portátiles institucionales que hagan uso de servicios de la Entidad como son: Establecer contraseñas de acceso robustas, cifrar la información almacenada, mantener el dispositivo con el sistema operativo siempre actualizado y con un antivirus activo.

✓ Si los funcionarios o contratistas hacen uso de aplicaciones móviles con información de la entidad en sus dispositivos personales, se deben tener en cuenta las condiciones descritas en el ítem anterior.

✓ Los funcionarios y contratistas no están autorizados a cambiar la configuración, ni la instalación/desinstalación de las aplicaciones móviles de los dispositivos móviles institucionales que se les entregue como recurso para la ejecución de sus obligaciones o funciones.

✓ Es responsabilidad del servidor público al que se le asignó el dispositivo móvil evitar la instalación de programas desde fuentes desconocidas, evitar el uso de redes inalámbricas públicas, y mantener desactivadas las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

13.2 Políticas teletrabajo

✓ Toda información gestionada por la ACI Medellín, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales con esta.

✓ La ACI Medellín establece los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos y contratistas de la entidad, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.

✓ La ACI Medellín establece el proceso de implementación de teletrabajo, de acuerdo con la normativa y los lineamientos exigidos, con el fin de proteger la información.

✓ El Subproceso de Gestión de Sistemas de Información debe garantizar los recursos necesarios para los teletrabajadores por tal motivo se da acceso en remoto del servidor acimed08, solo consulta sin permisos altos ni de superusuario al subproceso de Gestión Presupuestal y Financiera con el fin de poder realizar las consultas y transacciones de banco de manera segura y dentro de la red ACI.

13.3 Políticas de seguridad de los recursos humanos

✓ El subproceso de Gestión Humana realiza las verificaciones de los antecedentes (procuraduría, contraloría, policía) de los candidatos al cargo, la formación académica, experiencia y demás información que se requiera, de acuerdo con las leyes, reglamentos de la Entidad y ética pertinente.

✓ Todo servidor público y contratista recibe inducción y procesos periódicos de sensibilización en seguridad y privacidad de la información en la Entidad

✓ La ACI Medellín incorpora los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los Colaboradores y Terceros.

13.4 Políticas gestión de activos

✓ La ACI Medellín establece los métodos de identificación, clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades, manteniendo mecanismos acordes para el control de riesgos de la información.

✓ Los servidores públicos y contratistas deben hacer la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la Entidad.

✓ La ACI Medellín cuenta con un sistema o listado de equipos de cómputo portátil asignado a funcionarios o contratistas (Inventarios).

13.5 Políticas gestión de medios de almacenamiento

✓ Todo medio removible en estado de tránsito o préstamo deberá ser autorizado por el propietario del activo de información.

✓ Todo proceso para dar de baja o reutilización de dispositivos que contengan información almacenada, se debe proceder con la destrucción o borrado seguro.

✓ Cada medio removible de almacenamiento se identificará de acuerdo con la información contenida.

13.6 Políticas control de acceso y Manejo de la Información

✓ La ACI Medellín establece procedimientos para la creación de datos de acceso, suministro de accesos a la información, revisión periódica de los accesos otorgados, y desactivación o eliminación de las cuentas de usuario una vez finalizada la relación contractual.

✓ Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministradas de acceso a la red, sistemas de información, aplicaciones, entre otros.

✓ Todos los usuarios de sistemas de información deberán cambiar sus contraseñas de manera periódica. Las contraseñas son personales e intransferibles, y todo lo que ocurra en un sistema de información con determinado usuario, será responsabilidad de éste.

✓ Todos los servidores públicos y contratistas con acceso a un sistema de información o a la red informática institucional, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña y serán responsables de las acciones realizadas por el usuario que les ha sido asignado.

✓ Toda información institucional, debe manejarse a través de los correos electrónicos institucionales, el cual debe ser accedido desde equipos o dispositivos seguros.

✓ El acceso a Aplicativos Web de la entidad alojados en la nube, debe hacer desde equipos o dispositivos que briden las garantías suficientes de seguridad y responsabilidad del usuario, cualquier violación a la política de seguridad.

13.7 Políticas seguridad física y del entorno

✓ Los equipos de cómputo que pasen a un estado de retiro o requieran ser dados de baja deberán cumplir los siguientes lineamientos:

a. Al momento de retirar un equipo de la bodega (almacén), el subproceso de Gestión de Sistemas de Información realiza una copia de respaldo de la información almacenada en este activo.

b. el subproceso de Gestión de Sistemas de Información realiza el proceso de borrado seguro de la información almacenada en los equipos que van a ser cedidos o utilizados en la organización.

✓ Para todos los usuarios de las aplicaciones y sistemas de información de la ACI Medellín, es obligatorio que las sesiones sean cerradas al finalizar las actividades y no se deben dejar abiertas o desatendidas.

✓ Las áreas dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, cuentan con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

13.8 Políticas seguridad de las comunicaciones

✓ el subproceso de Gestión de Sistemas de Información realiza el bloqueo a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso institucional, mediante el uso de servidor proxy, firewall o control que mejor se ajuste a la necesidad.

✓ el subproceso de Gestión de Sistemas de Información asegura la protección de las redes y la transferencia de información. Para dar cumplimiento se deben firmar acuerdos de confidencialidad y de no divulgación entre la Entidad y entidades externas con las cuales se intercambie información e implementar controles de seguridad al monitoreo de la red.

✓ el subproceso de Gestión de Sistemas de Información implementa y mantiene la separación de las redes virtuales para garantizar la confidencialidad de la información en la red de telecomunicaciones de la Entidad.

✓ La transferencia de información deberá realizarse protegiendo la confidencialidad, integridad y disponibilidad de los datos de acuerdo con la clasificación del activo tipo información involucrada.

13.9 Políticas adquisición, desarrollo y mantenimiento de sistemas

✓ el subproceso de Gestión de Sistemas de Información busca que la Seguridad de la Información sea parte integral dentro ciclo de vida de desarrollo de los sistemas de información y en la adquisición de aquellos que presten servicios a la ACI Medellín, para ello establece los procedimientos del subproceso: mantenimiento preventivo y correctivo de equipos de cómputo, creación de usuarios y roles en los sistemas de información, copias de seguridad de información, soporte técnico a usuarios, identificación de activos de seguridad digital, con el fin de detectar vulnerabilidades antes de salir a producción y la aplicación de los procedimientos.

✓ el subproceso de Gestión de Sistemas de Información asegura que se diseñe e implemente los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.

✓ el subproceso de Gestión de Sistemas de Información establece controles técnicos para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información que son públicos mediante herramientas de seguridad perimetral de proveedores o de forma local.

✓ el subproceso de Gestión de Sistemas de Información cuenta con un ambiente de desarrollo y de pruebas seguro o, en su defecto, exige al proveedor mediante los contratos, que éste cuente con los controles de seguridad de la información sobre los ambientes.

✓ Los datos de pruebas que se utilicen durante todo el ciclo de vida de los sistemas de información deben ser seleccionados, utilizados y eliminados de forma segura.

13.10 Políticas gestión de incidentes

✓ el subproceso de Gestión de Sistemas de Información debe asegurarse que todos los servidores públicos y contratistas conozcan y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información. Por lo tanto, se debe establecer los mecanismos para registrar los incidentes el portal soporte Zoho con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

✓ el subproceso de Gestión de Sistemas de Información establece y ejecuta procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.

✓ el subproceso de Gestión de Sistemas de Información debe establecer los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

✓ el subproceso de Gestión de Sistemas de Información cuenta con una herramienta Zoho Analityc de los incidentes de seguridad de la información reportados y atendidos.

14. REFERENCIA NORMATIVA

- CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital.
- Decreto 103 de 2015 el cual reglamenta la ley 1712 de 2014 "Ley de Transparencia “.
- Ley 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013 y por el Decreto 1081 de 2015, “Protección de datos personales”.
- Decreto único reglamentario 1078 de 2015 – MinTic – Modelo de Seguridad y Privacidad de Información.
- ISO/IEC 27000:2013. Estándar del Sistema de Gestión de Seguridad de Información.
- Resolución 1519 de 2020: Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- Resolución 500 de 2021 Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de seguridad y privacidad de la información y el manual de políticas de seguridad de la información.
- Decreto 767 de 2022: "Por el cual se establecen los lineamientos generales de la

Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

15. RESUMEN DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE CAMBIOS
01	25/07/2018	Se crea el Plan de Seguridad y Privacidad de la Información
02	30/01/2019	Se hace revisión y actualización de todo el plan
03	24/01/2020	Se hace revisión y actualización de todo el plan
04	27/01/2021	Se hace revisión y actualización de todo el plan
05	19/01/2022	Se hace revisión y actualización de todo el plan
06	11/01/2023	Se hace revisión y actualización de todo el plan - Se incorpora seguridad y teletrabajo Se incorpora políticas según los lineamientos de la Mintic en la guía 8 y 9
07	15/01/2024	Se hace revisión y actualización de todo el plan - Se actualizan las actividades para la vigencia 2024 – Se incluye referencia normativa de acuerdo con la guía Minitic 2024

16. RESPONSABILIDAD Y AUTORIDAD

Elaboró / Actualizó:	Revisó:	Aprobó:
Nombre: Natalia Marcela Moná Roldán	Nombre: Luisa Fernanda Márquez Ruiz	Nombre: Cristina Zambrano Restrepo
Cargo: Auxiliar administrativo de Gestión de sistemas de información	Cargo: Directora Relaciones Administrativas	Cargo: representante legal