AGENCIA DE COOPERACIÓN E INVERSIÓN DE MEDELLÍN Y EL ÁREA METROPOLITANA

-ACI MEDELLÍN-

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CATALINA RESTREPO CARVAJAL

Directora Ejecutiva

ASTRID MADELEINE ÁLVAREZ

Subdirectora de Relaciones Administrativas

JOHN FABIO GÓMEZ GARCÍA

Auxiliar Administrativo de Sistemas e Informática

2018

CONTENIDO

INTRODUCCIÓN

La Agencia de Cooperación e Inversión de la Ciudad de Medellín y el Area Metropolitana ha reconocido la información como el activo más importantes de la entidad, haciendo necesaria la protección de la misma frente a factores de amenazas (externas) y debilidades (internas) que pueden poner en riesgo la misión y los objetivos instituciones, con este plan la ACI Medellín busca materializar una gestión responsable de la información que se genera en el desarrollo de sus procesos para garantizar la integridad, confidencialidad y disponibilidad de su mayor activo, estableciendo medidas de índole técnica y organizacional necesarias para avalar su seguridad en sistemas de información e infraestructura tecnológica, aplicando a todos los funcionarios y contratistas que interactúan con los recursos informáticos que pone a disposición la Agencia.

1 OBJETIVOS

1.1 Objetivo general

- Regular el uso adecuado de los sistemas de información y los recursos tecnológicos de la Agencia por parte de todos los funcionarios; 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 integridad, confidencialidad y disponibilidad.

1.2 Objetivos específicos

- Informar y concientizar a todos los funcionarios 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 en los sistemas de información.

2 ALCANCE

El plan de seguridad y privacidad de la información brinda 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.

3 TERMINOS Y DEFINICIONES

Confidencialidad: garantizar que la información sea accesible sólo por las personas autorizadas.

Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso 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.

Para los efectos de una correcta interpretación del presente plan, se realizan 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 hasta llamadas telefónicas.

✓ Routers: dispositivo de red de capa 3 diseñado para transportar 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 negación 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, Azureus, 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 o 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.

3 ROLES Y RESPONSABILIDADES

Comité Directivo: aprueban las Políticas de Seguridad y Privacidad Informática, es responsable de fortalecer e incentivar las políticas allí definidas dando cumplimiento a la gestión responsable frente a la información.

Usuarios Finales (funcionarios, contratistas, terceros): cumplir a cabalidad con las políticas de Seguridad y Privacidad informática, procedimientos y buenas prácticas que se tenga definido en la organización para el buen uso de los recursos tecnológicos. Informar cualquier anomalía, vulnerabilidad o incidente de seguridad que se detecte en el que hacer de sus labores

Auxiliar administrativo sistemas e informática: 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 formales a la subdirección 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 el buen cumplimiento de estas políticas. Sensibilizar al comité directivo de la Agencia la importancia de estas políticas de seguridad para el éxito de las mismas.

4 DIAGNOSTICO

En el año 2015 la ACI MEDELLÍN adopta dentro de su lista de manuales el de Políticas de Seguridad y privacidad informática aprobado y con el visto bueno desde el comité directivo, 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 Sistemas integrado de gestión se estipulo la guía 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. De la administración del riesgo se maneja también una matriz donde se identifican los riesgos desde cada proceso

aplicados a la información institucional y con las políticas de seguridad y este plan se busca mitigar al nivel más bajo.

5 DESCRIPCIÓN DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1 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.
- ✓ Todos los funcionarios que laboran para la ACI deben tener acceso sólo a la información necesaria para el desarrollo de sus funciones. Es responsabilidad del comité directivo solicitar el acceso de acuerdo con el trabajo realizado por el personal a su cargo.

  ✓ Las prerrogativas otorgadas para 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 es propiedad de la ACI.

5.2 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, entre otros.

- ✓ Todos funcionarios que utilice 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 confidencial y crítica.

- ✓ No se debe dejar visible sus contraseñas de correo, red y archivos, porque pueden ser utilizadas por otras personas alterando o dañando su información, ni tampoco comparta sus contraseñas pueden ser utilizadas con otros objetivos.

- ✓ No debe permitir que personal externo opere su información.

- ✓ Al desplazarse de su puesto de trabajo, bloquee la sección en el equipo, esto evita posibles ingresos no autorizados a su información.

5.3 Seguridad 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 caracteres siguientes:
  ✓ 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.

5.4 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 y los períodos de vigencia de las mismas, 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 de usuario desarrolle la administración de usuarios.

- ✓ El control de acceso 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.

- ✓ Todo sistema de información debe tener definidos los perfiles de usuario de acuerdo con la función y cargo que puedan acceder a dicho sistema.

- ✓ 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.

5.5 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 de tiempo real que accedan a la red interna de la entidad deben pasar a través de los sistemas de defensa electrónica 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. Todo se maneja desde el firewall perimetral Fortigate 90D.

5.6 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 ACI.

- ✓ 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.

5.7 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 los mismos, únicamente puede ser realizada por el personal del 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.

5.8 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 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 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.

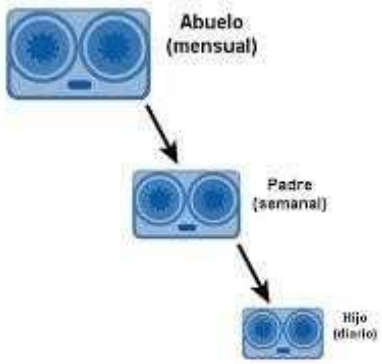
- ✓ No instalar (sincronizar) servicios de almacenamiento en la nube diferentes al OneDrive. Y mucho menos manejar información institucional en estos sistemas de almacenamiento.

- ✓ 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.

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



Descripción técnica

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 CD. 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.

Programación de copias de seguridad

En la Agencia 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 Veritas backup exec.

5.9 Soporte técnico

Todo requerimiento debe ser registrado mediante el portal de soporte, ubicado como acceso directo en el escritorio de cada usuario. Allí se debe ingresar con el usuario y contraseña asignado por el auxiliar administrativo en sistemas e informática. 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.

5.10 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 contrae.

Utilizar únicamente software autorizado e instalado por el auxiliar administrativo en sistemas e informática.

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

5.11 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 en sistemas e informática.
- ✓ 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 del proceso.
- ✓ Por ningún motivo el usuario instalara software de promoción y entretenimiento.
- ✓ La adquisición o desarrollo de software será responsabilidad del auxiliar administrativo en sistemas e informática.

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

Recomendaciones y 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 del correo electrónico

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 alguien externo y ajeno 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 su(s) autor(es).

-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 Agencia 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.

6 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 proceso 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 diferentes a las personales.
- ✓ 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 colectar 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, salesforce CRM institucional, sistema Veritas backup exec, unidad de red no autorizada.
- ✓ 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. P

7 PROPIEDAD INTELECTUAL

La ACI Medellín podrá tener acceso en el momento que sea necesario a cualquier información alojada en alguno de los equipos que son propiedad del mismo tales como PC, servidores, unidades lógicas de la SAN entre otros, así mismo podrá tener acceso a cualquier información generada y transmitida por la red.

Todos los computadores y servidores de la Agencia 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 e informática 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.

8 TRATAMIENTOS DE DATOS PERSONALES

La ACI Medellín dentro de sus manuales tiene el de tratamiento de datos personales en atención al objeto 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 las informaciones que se hayan 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, adopta este manual de políticas para el tratamiento de datos personales que obtenga y administre en desarrollo de su objeto social, 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.

9 ACTIVIDADES VIGENCIA 2018 II

El subproceso de recurso tecnológicos 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.

-El activo más importante para la ACI Medellín su información, requiere para la operación del subproceso realizar una actualización del inventario de activos tecnológicos.

-En las inducciones de funcionarios nuevos y contratista se le socializa las políticas de seguridad y privacidad de la información haciendo énfasis en su importancia tanto para el usuario como para la entidad, es necesario volver a dar a conocer las políticas 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.

-Identificar activos críticos que pongan en peligro la información de la entidad mitigando los riesgos de seguridad identificados en el sistema integrado de gestión.

10 CRONOGRAMA DE ACTIVIDADES

N°	ACTIVIDAD	RESPONSABLE	FECHA INICIO	FECHA FIN	Entregable
1	Actualizar inventario activo tecnológicos	Auxiliar Administrativo Sistemas e Informática	3 septiembre 2018	30 de septiembre 2018	Documento inventario actualizado
2	Reunión con cada proceso	Auxiliar Administrativo Sistemas e Informática	1 octubre 2018	31 de octubre 2018	Acta de reunión
3	Identificar proveedores críticos	Auxiliar Administrativo Sistemas e Informática	27 agosto 2018	31 agosto 2018	Procedimiento de supervisión, Políticas de operación
4	Identificar activos críticos	Auxiliar Administrativo Sistemas e Informática	19 noviembre	23 noviembre	Documentos Activos críticos

11 RESUMEN DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE CAMBIOS
1	25/07/2018	Se crea el plan PETI