MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA SOLUCIÓN TECNOLÓGICA DE LA AGENCIA PARA LA GESTIÓN DEL PAISAJE, EL PATRIMONIO Y LAS ALIANZAS PÚBLICO PRIVADAS - APP

ENERO 2024
Medellín

Tabla de Contenido

Fecha	Versión	Realizado por	Descripción
15 de enero de 2024	2.0	Andrés Mauricio Moreno Álvarez	Definir e implementar las políticas de seguridad informática que dan las pautas y rigen para la gestión, el uso adecuado y la seguridad de la información de los sistemas informáticos y en general, sobre el ambiente tecnológico de la AGENCIA APP

1. INTRODUCCIÓN

La Seguridad Informática se basa en la existencia de un conjunto de directrices que brinden instrucciones claras y oportunas, soportando la gestión de la Alta Dirección frente al gran dinamismo de nuevos ataques y violaciones a la seguridad e integridad de la información.

Este documento se debe entender como el compendio de reglas que permiten definir la gestión, protección y asignación de los recursos corporativos, acorde a los lineamientos de la Alta Dirección, concientizando a cada uno de los miembros acerca de la importancia y sensibilidad de la información propia de la organización.

Todas las directrices contempladas en este documento deben ser revisadas periódicamente, determinando oportunamente la creación, actualización y obsolescencia de cada directriz, con el fin de mitigar las vulnerabilidades identificadas y mantener altos estándares de seguridad para la AGENCIA APP.

En términos generales estas políticas de seguridad de información, propende por englobar los procedimientos más adecuados, tomando como lineamientos principales cuatro criterios, que se detallan a continuación:

Seguridad Organizacional: Dentro de este, se establece el marco formal de seguridad que debe sustentar la AGENCIA APP, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

Seguridad Lógica: Trata de establecer e integrar los mecanismos y procedimientos, que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

Seguridad Física: Identifica los límites mínimos que se deben cumplir en cuanto a perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en la importancia de los activos.

Seguridad Legal: Integra los requerimientos de seguridad que deben cumplir todos los funcionario, contratistas, colaboradores y usuarios de la red institucional bajo la reglamentación de la normativa interna de la AGENCIA APP, en cuanto al recurso humano, tendrá sanciones aplicables ante faltas cometidas de acuerdo con la Ley o la normativa interna estipulada.

2. PRÓPOSITO

Este documento tiene como finalidad dar a conocer las PSI - Políticas de Seguridad de la Información y ESI - Estándares de Seguridad Informática, que deben aplicar y acatar todos y cada uno de los funcionarios, contratistas, colaboradores y usuarios de la AGENCIA APP, enfocada en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Teniendo en cuenta la existencia de una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información, con el fin de establecer en el interior de la entidad una cultura de calidad operando en una forma confiable. La responsabilidad por la seguridad de la información no depende únicamente de la Dirección Técnica o el Área de Tecnología Informática y Comunicaciones, sino que es una responsabilidad de cada funcionario, contratista, colaborador y usuario activo de la entidad.

3. ALCANCE

El alcance de las políticas y estándares contemplados en este manual aplican a:

- Todas las Áreas de la AGENCIA APP por su condición de gestoras, procesadoras y protectoras de todo tipo de información soportada en cualquier medio físico impreso o electrónico de la Entidad.

- Todos los funcionarios, contratistas, colaboradores y usuarios activos de la AGENCIA APP, y todo el personal tercero, que hagan uso de los sistemas de información, plataformas y servicios tecnológicos de la entidad.

- Esta política es aplicable también a todo el equipo y servicios propietarios o arrendados que de alguna manera tengan que utilizar local o remotamente el uso de la Red o recursos tecnológicos de la AGENCIA APP, así como de los servicios e intercambio de archivos y programas.

4. OBJETIVOS

- Establecer los criterios y comportamientos que deben seguir todos los funcionarios, contratistas, colaboradores y usuarios de la AGENCIA APP, con el fin de velar por la adecuada protección, preservación y salvaguarda de la información y de los sistemas corporativos, respondiendo a los intereses y necesidades organizacionales y dando cumplimiento a los 3 principios de la gestión de la información: **Confidencialidad, Integridad y Disponibilidad**, acogidos de la mejores prácticas de gestión de la información, implícitas en el estándar internacional ISO/IEC-27001:2005.

- Difundir las políticas y estándares de seguridad informática a todo el personal de la AGENCIA APP, para que sea de su conocimiento y cumplimiento en los recursos informáticos utilizados o asignados y establecer las responsabilidades, principios, criterios, directrices y conductas dentro de los lineamientos de la ética y el buen gobierno de la AGENCIA APP.

- Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la AGENCIA APP.

5. VIGENCIA

Todas las amenazas están en continuo proceso de expansión, lo que, unido al progresivo aumento de los sistemas de información y dependencia del negocio, hace que todos los sistemas y aplicaciones estén expuestos a riesgos cada vez mayores, que, sin una adecuada gestión de los mismos, pueden ocasionar que su vulnerabilidad se incremente y consiguientemente los activos se vean afectados. Todo funcionario, contratista, colaborador y usuario de La AGENCIA APP, es responsable del cumplimiento de los estándares, directrices y procedimientos de control de acceso, así como también de notificar a su nivel jerárquico superior, cuando por algún motivo no pueda cumplir con las Políticas de Seguridad indicando el motivo por el cual no le es posible apegarse a la normativa de seguridad. Cabe destacar que este nivel de responsabilidad va a ser conocido por las diferentes áreas de La AGENCIA APP, quien será el garante de que esta información sea conocida por cada integrante de área.

La documentación presentada como Políticas de Seguridad entrará en vigencia desde el momento en que sean revisadas por el Comité Institucional la Dirección Técnica y aprobadas por la Dirección General. Esta normativa deberá ser revisada y actualizada conforme a las exigencias de la AGENCIA APP o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica.

6. NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

Es de carácter obligatorio para todo el personal, la notificación inmediata de algún problema o violación de la seguridad, del cual fuere testigo; esta notificación debe realizarse por escrito o vía correo electrónico a la Dirección Técnica y/o al Área de Tecnología Informática y Comunicaciones, quienes están en la obligación de realizar las gestiones pertinentes al caso y de ser cierta la sospecha, tomar las medidas adecuadas para solucionar el incidente.

Es responsabilidad de los servidores contratistas, y usuarios de la AGENCIA APP que manejen datos o información a través de accesos debidamente autorizados, el cumplimiento de las políticas de control de acceso, puesto que estas descansan en el establecimiento de responsabilidades donde se incurra en alguna violación en materia de seguridad acarreando sanciones a quien las haya causado, toda vez que esto

ocasionaría perjuicios económicos a la AGENCIA APP de diversa consideración. Es por ello que las personas relacionadas de cualquier forma con los procesos tecnológicos deben ser conscientes y asumir que la seguridad es asunto de todos y, por tanto, se debe conocer y respetar las Políticas de Seguridad.

Está fundamentado como una exigencia que el personal de la entidad conozca sus responsabilidades, sanciones y medidas a tomar al momento de incurrir en alguna violación o falta escrita en las Políticas de Seguridad. Por esta razón se entenderá que sólo una adecuada política de seguridad tecnológica apoyará la concientización para obtener la colaboración de los empleados, funcionario, contratistas, colaboradores y usuarios de la AGENCIA APP, haciéndoles conscientes de los riesgos que podemos correr y de la importancia del cumplimiento de las normas.

7. SANCIONES POR INCUMPLIMIENTO

Estas políticas son obligatorias de cumplir en cada nivel de la entidad, por lo tanto, deben ser cumplidas por (funcionario, contratistas, colaboradores y usuarios) y todo tercero que interactúe con la Información, los Sistemas de Información y demás Activos Informáticos de la AGENCIA APP.

En el evento en que se evidencia la transgresión o incumplimiento de cualquier política o estándar contemplado en este documento, se debe considerar como una falta disciplinaria y deberá iniciar una investigación interna y en caso necesario se aplicarán las sanciones contempladas en la Ley 734 de 2002 y demás normas complementarias que la adicionen o modifiquen.

8. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Dirección Técnica de la AGENCIA APP, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con el objeto, misión y visión de La AGENCIA APP.

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

De acuerdo con lo anterior, esta política aplica a la AGENCIA APP, según como se define en el alcance, sus funcionarios, contratistas, colaboradores, terceros, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función pública y administrativa.
- Mantener la confianza de los ciudadanos y servidores o contratistas.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, terceros y ciudadanos de la AGENCIA APP.
- Garantizar la continuidad de la prestación del servicio frente a incidentes.
- La AGENCIA APP ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros conforme a las necesidades de la entidad, y a los requerimientos regulatorios.

A continuación, se establecen los principios de seguridad que soportan el Sistema de Gestión de la Seguridad de la Información – SGSI de la AGENCIA APP:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas, ciudadanos y terceros

- La AGENCIA APP, protegerá la información generada, procesada o resguardada por los procesos, proyectos, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o ciudadanos), o como resultado de un servicio interno en outsourcing.

- La AGENCIA APP, protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- La AGENCIA APP, protegerá su información de las amenazas originadas por parte del personal funcionario o contratista.

- La AGENCIA APP, protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- La AGENCIA APP, controlará la operación de sus procesos de gestión garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- La AGENCIA APP, implementará control de acceso a la información, sistemas y recursos de red.

- La AGENCIA APP, garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La AGENCIA APP, garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- La AGENCIA APP, garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

9. PRACTICAS INSTITUCIONALES

9.1. Derechos y deberes del Usuario (funcionario o contratista)

Si un funcionario o contratista de la AGENCIA APP, no está en la capacidad del manejo de las herramientas y programas que se utilizan en la entidad, este, debe solicitar por medio de un correo electrónico la capacitación respectiva, con el fin de que sus funciones o la prestación del servicio se reflejen al máximo.

Es responsabilidad de los usuarios (funcionarios y contratistas) almacenar la información correspondiente a la AGENCIA APP, únicamente en Google Drive, lugar asignado por la entidad. La información personal se puede grabar en la unidad de disco del equipo generalmente C:\, Es de anotar que la AGENCIA APP, no se hace responsable de la información personal del usuario.

Es importante tener en cuenta las siguientes recomendaciones:

- En el momento que se esté operando el equipo de cómputo no se debe consumir comidas ni bebidas.

- Evitar cubrir el Computador o Portátil con objetos que obstruyan la ventilación.

- El Computador o Portátil no debe estar sobre una superficie húmeda, tampoco debe estar en el suelo o un lugar donde se mueva de manera constante.

- El usuario no podrá cambiar de lugar el Computador de escritorio, este procedimiento lo debe solicitar de manera previa, al área de Tecnología Informática y Comunicaciones.

- El usuario tiene la responsabilidad de mantener los cables de conexiones eléctricas y red en buen estado, no pisarlos ni ponerles objetos encima, también tiene la responsabilidad de informar al Área de Tecnología Informática y Comunicaciones si algunos de estos complementos fallan.

- Los equipos de cómputo solo deben ser abiertos por el personal del Área de Tecnología Informática y Comunicaciones o en consecuencia por el proveedor asignado por la Dirección Técnica.

- Los equipos de cómputo solo deben ser reparados por el personal del Área de Tecnología Informática y Comunicaciones o en consecuencia por proveedor asignado por la Dirección Técnica.

- Al equipo de cómputo, periférico o accesorio de tecnología de información que sufra algún desperfecto, daño por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de políticas de seguridad, dando cumplimiento al debido proceso en caso de ser necesario y reportado al Área de Gestión Humana

- El funcionario o contratista que tenga bajo su responsabilidad o asignado algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normativa vigente en los casos de robo, extravío o pérdida del mismo.

- El préstamo de equipos de cómputo deberá ser solicitados al Área de Tecnología Informática y Comunicaciones, previa autorización del superior jerárquico, la Dirección Técnica o supervisor. Se evaluará el tipo de seguro que se tiene con el equipo y precisará si es posible el préstamo para retirarlo de las instalaciones de la AGENCIA APP.

- En el caso que se presenta pérdida o robo del equipo de Cómputo (Portátil y PC de escritorio), el funcionario o contratista deberá dar aviso inmediato a la Dirección Técnica, de la desaparición, robo o extravío de equipos de cómputo bajo su responsabilidad.

- Los usuarios de la Agencia APP, tienen la obligación de proteger la información utilizada en la infraestructura tecnológica que presta servicio a la oficina. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna institucional a otras dependencias alternas o redes externas como internet.

9.2. Empleados o Contratistas Nuevos

Toda persona que ingrese como empleado o contratista a La AGENCIA APP, tendrá la posibilidad de hacer uso de los servicios informáticos de la entidad, acatando las cláusulas de confidencialidad y el uso adecuado de los recursos informáticos (Equipos informáticos propios o ajenos, información documental de la Agencia, Páginas WEB de la Agencia, Intranet perteneciente a la Agencia, Usuarios de correo electrónico y claves asignadas), conforme se establece en el contrato, acta de posesión o documentos adicionales.

Además de lo anterior, los usuarios de la AGENCIA APP, tienen la responsabilidad de cumplir con las políticas y recomendaciones de seguridad informática que se presenta en este documento.

Los usuarios de la AGENCIA APP, serán capacitados sobre las políticas y estándares de seguridad informática y se le enviará el manual de usuario en donde se plasman las obligaciones y sanciones a las que estará expuesto en caso de incumplirlas.

El funcionario o contratista de la AGENCIA APP, deberá cuidar de todo daño, los equipo y las instalaciones de la entidad, también el cuidado de la información, esta no puede ser divulgada, debe permanecer en reserva o confidencial, dando aplicación a la normativa vigente y las cláusulas del contrato o funciones como servidor público.

En el caso que un funcionario o contratista de la AGENCIA APP, detecte un caso de riesgo que afecte los equipos de cómputo, las telecomunicaciones, debe reportarlo de inmediato a la Dirección Técnica y/o el Área de Tecnología Informática y Comunicaciones.

9.3. Unidad de Almacenamiento de la Información y Equipos de Cómputo.

La administración de las unidades de almacenamiento de la información, sólo estarán a cargo de la Dirección Técnica y/o el Área de Tecnología Informática y Comunicaciones, ningún usuario, o contratista de la AGENCIA APP, podrá tener rol de administrador para estas unidades.
La solicitud de permisos de acceso a las unidades de almacenamiento de la información, sólo se podrá realizar previa notificación de su superior jerárquico o supervisor; NO se concederán permisos a ningún usuario y/o empleado sin recibir dicha notificación.

El centro de cómputo, Servidores, Switches, Router, Modem y planta telefónica, solo podrán ser manipulada y accedida por el Área de Tecnología Informática y Comunicaciones.

Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, tampoco podrán instalar software no autorizados, ni retirar sellos de los mismos sin la autorización de la Dirección Técnica, en caso de requerir dicho proceso de solicitará por medio de un correo electrónico.

9.4. Backup

Los usuarios deberán asegurarse de respaldar la información propiedad de la AGENCIA APP en la carpeta de Google Drive asignada a cada persona, en caso de ser necesario enviar el equipo a reparación, este se debe entregar sin ninguna información, previendo así la pérdida involuntaria de información o distribución inadecuada de la misma.

Cada funcionario o contratista es responsable directo de la generación de los Backup o copias de respaldo.

9.5. Seguridad Informática

Los funcionarios o contratistas de la AGENCIA APP que utilizan los computadores, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red y demás amenazas informáticas que existen en el medio.

La Dirección Técnica y el Área de Tecnología Informática y Comunicaciones, es la encargada de establecer las políticas y procedimientos administrativos para regular, controlar y describir el acceso de visitantes, funcionarios o contratistas no autorizados a la red interna, para así evitar daños en los sistemas informáticos de la AGENCIA APP.

Cuando un funcionario o contratista no autorizado o un visitante requieran ingresar a la red de la Agencia APP, debe solicitar mediante comunicado interno debidamente firmada y autorizado por el Jefe inmediato de su sección o dependencia, se debe especificar el tipo de actividad a realizar.

Los equipos de cómputo principal de la AGENCIA APP, (Switches, Servidores, equipo WIFI, Planta Telefónica), deben ser administrados solo por el Personal Tecnología Informática y Comunicaciones.

Cuando se vaya a realizar un mantenimiento en algunos del equipo antes mencionados, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.

9.6. Adquisición de Software

Los usuarios que requieran la instalación de software en la AGENCIA APP, deberán justificar su uso y solicitar su autorización al Área de Tecnología Informática y Comunicaciones, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que será usado.

Se considera una falta grave el que los usuarios o funcionarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la AGENCIA APP, que no esté autorizado por la Dirección Técnica.

La Dirección Técnica, debe mantener informado a todo el personal de la AGENCIA APP, las políticas contra la piratería de software, utilizando todos los medios de comunicación disponibles: Página WEB, Email y Boletines, también la publicación de las sanciones o multas a las que la AGENCIA APP, incurre en caso de incumplimiento.

La AGENCIA APP, posee contratos de compra y uso de Software con varios proveedores, esto garantiza en gran medida la legalidad de los programas adquiridos. En el momento que sea necesario otro "software",

será adquirido con el cumplimiento de la normativa contractual con el Proveedor debidamente certificado, el cual deberá entregar al momento de la compra, el programa y la licencia del software con toda la documentación pertinente y necesaria que certifique la originalidad y validez del mismo.

El control de manejo para las licencias será responsabilidad del área de Tecnología Informática y Comunicaciones en cabeza de la Dirección Técnica.

El Área de Tecnología Informática y Comunicaciones, tomará todas las precauciones cuando se vaya a realizar una reinstalación de un programa, borrando completamente la versión instalada para luego proceder a instalar la nueva versión que desea, esto siempre y cuando no sea una actualización del mismo.

El Área de Tecnología Informática y Comunicaciones mantendrá un inventario de equipos físicos y de los programas instalados de acuerdo a la necesidad de la AGENCIA APP, así como también tiene la obligación de desinstalar programas no autorizados o no legalizados, llevando igualmente un inventario de ello.

El Área de Tecnología Informática y Comunicaciones, tiene establecido que los funcionarios no están autorizados para instalar ningún tipo de programas en los equipos pertenecientes a la AGENCIA APP, cada tres meses se realizará un inventario físico de los programas instalados en cada uno de los computadores de la AGENCIA APP.

9.7. Administración de la Red

Los funcionarios y contratistas de la AGENCIA APP, no están autorizados para realizar conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando ningún tipo de protocolo de transferencia de archivos, dentro de la infraestructura de red de la AGENCIA APP, sin la autorización del área de Tecnología Informática y Comunicaciones.

9.8. Seguridad para la red

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Dirección Técnica y/o el Área de Tecnología Informática y Comunicaciones, en la cual los funcionarios o contratistas realicen la exploración de los recursos informáticos en la red de la AGENCIA APP, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad al igual que la creación de conexiones remota no autorizadas

9.9. Administración de Correo electrónico

Los funcionarios o contratistas solo deben usar cuentas de correo electrónico Institucional, no deben manipular cuentas de correo pertenecientes a otro funcionario o contratista. Si fuera necesario leer el correo

de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re-direccionar el correo a otra cuenta de correo interno.

Los funcionarios y contratistas deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de la AGENCIA APP. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

Los funcionarios y contratistas podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando sea enviado de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones, actividades y responsabilidades.

No está autorizado falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico, quien lleva a cabo esta práctica incurre en una falta ante la entidad con base en las políticas de seguridad de la AGENCIA APP.

9.10. Internet

El acceso a Internet provisto por la AGENCIA APP, a los usuarios y visitantes se debe utilizar exclusivamente para las actividades relacionadas con las necesidades del cargo, servicio y funciones desempeñadas.

Cualquier acceso a Internet tienen que ser realizados a través de los canales de acceso provistos por la AGENCIA APP, en caso de necesitar una conexión a Internet alterna o especial, ésta debe ser notificada y aprobada por la Dirección Técnica y/o el área de Tecnología Informática y Comunicaciones.

Cuando se presente un incidente de inseguridad vía WEB, los usuarios de la AGENCIA APP deben reportarlo al área de Tecnología Informática y Comunicaciones de inmediato después de su identificación, así se verificará si se trata de un incidente de seguridad informática.

Cuando los funcionarios y contratistas de la AGENCIA APP, acceden a los servicios Web de la AGENCIA APP, están aceptando que:

I. Serán sujetos de monitoreo de las actividades que realiza en Internet, conocen que existe la prohibición al acceso de páginas no autorizadas y que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
II. Saben que existe la prohibición de descarga de software sin la debida autorización del área de Tecnología Informática y Comunicaciones
III. La utilización de Internet es para el desempeño de sus funciones y actividades en la AGENCIA APP y no para propósitos personales.

10. POLITICAS Y ESTANDARES DE SEGURIDAD DE LA INFORMACIÓN

10.1. Gestión de contraseñas

a. Para garantizar la seguridad tanto de la información como de los equipos, el Área de Sistemas o Tecnología Informática asignará a cada usuario las claves de acceso que dé lugar: acceso al computador, acceso a la red interna, acceso al correo electrónico, acceso a las aplicaciones correspondientes.

b. La autorización para la creación, eliminación o modificación de perfiles de acceso es responsabilidad Dirección Técnica y/o del área de Tecnología Informática y Comunicaciones, Administrador de cada aplicación.

c. Los usuarios no deben tener acceso a opciones del Sistema de Información que no utilicen.

d. El Área Tecnología Informática y Comunicaciones, administradores de las aplicaciones, responsables de activos tecnológicos y los dueños de la Información serán los responsables de velar por que los perfiles de acceso existentes sean acordes con las funciones realizadas por cada uno de los usuarios.

e. En el evento que algún usuario deje de tener vínculo laboral o contractual con la entidad, el Área de Gestión Humana deberá notificarlo por escrito al Área de Tecnología Informática y Comunicaciones, con la finalidad de inactivar todas las cuentas y accesos, equipos y recursos informáticos asignados.

f. En el evento que algún usuario olvide, bloquee o extravíe su contraseña, debe informarlo a su superior jerárquico o supervisor, para que autorice la modificación del perfil de acceso de dicho usuario.

g. Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica de la AGENCIA APP, deberá ser notificada al Área de Tecnología Informática y Comunicaciones para que se tomen las medidas necesarias.

10.2. Uso de Contraseñas

a. Las contraseñas establecidas, deben cumplir con los parámetros mínimos contemplados para contraseñas fuertes o de alto nivel:

- Debe ser de mínimo ocho caracteres alfanuméricos de longitud.

- Debe contener como mínimo cuatro letras, de las cuales una debe ser Mayúscula.
- Debe contener mínimo cuatro números.
- Debe contener como mínimo un carácter especial (+-*/@#$%&). No debe contener vocales tildadas, ni eñes, ni espacios.
- No permitir repetir las últimas 6 claves utilizadas.

b. Las contraseñas deben ser cambiadas cada 3 meses, o cuando lo considere necesario debido a alguna vulnerabilidad en los criterios de seguridad.

Recomendaciones

A continuación, se relaciona una lista de aquellas actividades que **NO** se deben realizar respecto de las claves:

- Las claves deben ser de fácil recordación.
- NO deben ser basados en información personal, ni fechas especiales.
- NO escriba y guarde las claves en ningún lugar de su oficina, en papeles, agendas u otro medio físico.
- NO de su clave o haga alusión al formato de su clave, con compañeros de trabajo cuando este en vacaciones.
- NO hable o revele sus claves enfrente de otros, en el teléfono, a su jefe, supervisor, miembros de su familia, ni permita que nadie vea cuando digita la clave en un computador.
- NO revele su clave en un mensaje de correo electrónico, ni utilice la característica “recordar contraseña” de ninguna aplicación (ej.: Outlook, Internet Explorer, Gmail).
- Las claves nunca se deben almacenar en un servidor o máquina en red sin utilizar algún tipo de encriptación.
- NO utilice su clave en un computador que considera no confiable.

10.3. Seguridad de la Información

Gestión de la Información: Su objetivo es garantizar el adecuado uso, protección, confidencialidad, integridad y disponibilidad de la Información de la entidad. Aplica para todos los usuarios de componentes de la plataforma tecnológica de la AGENCIA APP.

Ubicación

a. Debe existir dentro de la configuración de todos los equipos informáticos, una partición, destinada para el almacenamiento de la información de usuario.

b. Se debe crear una estructura tipo árbol, estandarizada, para el almacenamiento y gestión de la información de usuario, la cual será parametrizada para optimizar la generación automática de Copias de Seguridad. La estructura debe estar acorde a lo definido en los protocolos de configuración de equipos establecidos por el Área Tecnología Informática y Comunicaciones.

c. El usuario no debe almacenar información directamente en los escritorios del sistema operativo, por ser una ubicación alojada en la partición base del disco duro, esto puede ocasionar que se pierda cuando sea necesario la reinstalación de software en caso de reparación o recuperación del sistema o por el contrario sea susceptible a accesos y modificaciones no autorizados, por lo tanto, se recomienda que sean creados accesos rápidos en el escritorio a los archivos de permanente consulta.

Clasificación

a. La información se debe clasificar de acuerdo con su criticidad y origen, que permitan el uso y acceso de forma fácil y oportuna. La información personal del usuario, no es considerada crítica, su almacenamiento será designado claramente en un directorio especial y estará sujeto a auditabilidad.

b. Todos los empleados y contratistas que conforman las diferentes áreas deben clasificar la información que tengan bajo su custodia.

c. Todo archivo debe ser almacenado en la estructura y ubicación destinada para tal fin, bajo algún mecanismo de nemotecnia o identificación que permita su fácil acceso.

d. La información pública debe tener una estructura definida por los responsables de la misma, y divulgada oportunamente a los interesados.

e. Toda la información utilizada por los usuarios de la AGENCIA APP, es de la entidad y por lo tanto el uso inadecuado de la misma es responsabilidad el usuario.

10.4. Administración de archivos

a. Todo usuario que utilice los recursos informáticos, tiene la responsabilidad de velar por la integridad, **confidencialidad, disponibilidad, y auditabilidad** de la información que maneje, especialmente si dicha información ha sido clasificada como crítica.

b. Los archivos creados por los usuarios deben ser confidenciales, de manera que no sean compartidos por los demás usuarios de la entidad sin previa autorización.

c. Se debe mantener y compartir únicamente la información que el usuario elija, previa confirmación con el Área Tecnología Informática y Comunicaciones. La integridad de toda información compartida entre usuarios, es responsabilidad de los mismos.

d. Los archivos administrativos que se utilizan en procesos institucionales o equipos de cómputo que requieran una clave o contraseña especial, ésta debe ser notificada y solicitada al Área de Tecnología Informática y Comunicaciones

e. Toda la información de los usuarios debe contar con copias de respaldo para garantizar su disponibilidad, seguridad y recuperación.

f. El acceso no autorizado a los sistemas de información y uso indebido de los recursos informáticos de la entidad está prohibido. Se considera que hay uso indebido de la información y de los recursos, cuando el usuario incurre en cualquiera de las siguientes conductas:

- Suministrar o hacer pública la información sin la debida autorización, o usar la información con el fin de obtener beneficio propio o de terceros.
- Hurtar software de la AGENCIA APP (copia o reproducción entre usuarios).
- Copiar un producto informático de la AGENCIA APP.
- Intentar modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos sin la debida autorización.
- Transgredir o burlar los mecanismos de autenticación u otros sistemas de seguridad.
- Utilizar la infraestructura de la AGENCIA APP, (computadores, software, información o redes) para acceder a recursos externos con propósitos ilegales o no autorizados.
- Descargar o publicar material ilegal, con derechos de propiedad o material nocivo usando un recurso de la AGENCIA APP.
- Uso personal de cualquier recurso informático de la AGENCIA APP, para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material pornográfico.
- Violar cualquier Ley o Regulación nacional respecto al uso de sistemas de información.

10.5. Confidencialidad de archivos

a. La información de la AGENCIA APP no podrá ser extraída de las instalaciones, sin previo conocimiento y autorización por parte de la Dirección General, Dirección Técnica y Subdirecciones.

b. Antes de entregar información a terceros se debe hacer una evaluación de esta, con el fin de determinar si la información solicitada se debe entregar o no.

c. En los contratos con terceros se debe incluir una cláusula de confidencialidad, la cual prohíba la divulgación personal o a medios de comunicación la información de la AGENCIA APP.

d. Todo usuario mantendrá total confidencialidad sobre la información a que tenga acceso y no la utilizará con propósitos distintos a los determinados en razón de su cargo. Si se requiere copiar información sensible, se debe contar con una autorización del personal designado por la Dirección Técnica.

10.6. Confidencialidad de datos de funcionarios y/o contratistas

a. Toda la información personal de los funcionarios y contratistas tal como nombres, direcciones, teléfono, datos familiares, y demás existentes, debe ser de uso restringido, respetando la privacidad de la persona, si dicha información se requiere por la entidad, debe solicitarse el permiso de divulgación y entrega de dicha información al empleado y/o contratista.

b. Si la AGENCIA APP cuenta con una aplicación o software de hojas de vida, la información allí almacenada debe ser de uso restringido, únicamente podrá ser divulgada con la autorización del empleado o contratista.

a. Todo vínculo con los empleados, funcionarios, contratistas, debe contemplar, una autorización de tratamiento de su información, que garantice la confidencialidad, integridad y disponibilidad de la misma, a que tenga lugar por la naturaleza de su relación contractual.

b. La información funcionarios, contratistas no podrá ser divulgada o entregada a menos que el empleado, funcionarios, contratistas lo autorice, debe ser tratada bajo los lineamientos establecidos en el Manual de Políticas y Procedimientos de Protección de Datos Personales de la AGENCIA APP

11. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Se busca establecer la función de administración de Seguridad Informática de la AGENCIA APP. Aplica a la Dirección General, Dirección Técnica, Subdirecciones, Sistemas y Usuarios.

Planificación

La AGENCIA APP, debe adoptar en lo posible, las buenas prácticas en seguridad de la Información, mediante la generación de políticas y procesos estructurados de planificación y capacidad en Tecnologías de Información y Comunicaciones, desarrollo seguro y pruebas de seguridad.

11.1. Administración de la Seguridad de la Información:

a. El Área Tecnología Informática y Comunicaciones, será responsable de la administración de la seguridad informática, y debe velar por el cumplimiento de las políticas, normas y procedimientos relacionados con Seguridad Informática, así como de planear y coordinar todos los proyectos relacionados con la implantación de controles para optimizar y mejorar continuamente la seguridad de la información de la entidad.

b. La Dirección Técnica, debe avalar las tareas de administración de Seguridad Informática de los activos tecnológicos, dentro de las cuales se deben comprender como mínimo: definición de accesos, administración de cuentas, definición de perfiles de usuarios y administradores y atención de incidentes de seguridad informática.

Procedimientos de operación:

El Área Tecnología Informática y Comunicaciones, debe mantener documentados todos los roles y responsabilidades, procesos, procedimientos, normas y directrices de seguridad de la información, alineadas con las premisas contempladas en las Políticas de Seguridad de la Información, de la AGENCIA APP.

Evaluación y tratamiento de riesgos

a. La AGENCIA APP, debe garantizar la evaluación periódica de los riesgos inherentes a la gestión y seguridad de la información, para lo cual se apoyará en auditorías internas, fundamentadas en metodologías y métodos documentados, estructurados y generalmente aceptados, que avalen la adecuada gestión de la Información.

b. El Área Tecnología Informática y Comunicaciones, debe evaluar los riesgos identificados y la tolerancia al riesgo, para determinar su tratamiento y documentación en un Plan de Tratamiento de Riesgos - PTR.

Responsabilidad de la Dirección

La Dirección Técnica debe revisar, evaluar y aprobar las políticas de seguridad de la información propuestas por el Área Tecnología Informática y Comunicaciones.

Responsabilidad de Tecnología

a. El Área Tecnología Informática y Comunicaciones, es responsable por la asignación y administración de activos informáticos requeridos por los usuarios para el cumplimiento de sus labores.

b. El Área Tecnología Informática y Comunicaciones es responsable por la custodia de la información en servidores, redes, medios de almacenamiento y medios digitales.

Responsabilidad de propietarios, custodios y usuarios de la información:

a. El usuario es responsable por la creación, administración y tratamiento de la información a su cargo.

b. Es responsabilidad de los usuarios de activos tecnológicos de la AGENCIA APP:

- Administrar la información a su cargo, y mantener en forma organizada la información existente en el computador personal a su cargo.

- Hacer uso adecuado de la información de propiedad de la AGENCIA APP y garantizar la integridad, veracidad, disponibilidad y confidencialidad de la información asignada para el cumplimiento de sus funciones, y velar por el adecuado almacenamiento de la información.

- Utilizar correctamente las contraseñas, y mantener la confidencialidad de las mismas.

- Reportar al Área de Sistemas o TI, cualquier incidente de seguridad que se presente en su equipo, o que sea percibido en la información usada en las labores diarias.

- Hacer uso racional de los recursos informáticos provistos por la AGENCIA APP.

- Conocer y cumplir cabalmente las políticas, normas, procedimientos y estándares definidos por la AGENCIA APP.

12. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DE LOS RECURSOS

Gestión de los activos, Garantizar un adecuado uso de la Infraestructura (Software y Hardware) de cómputo de la AGENCIA APP, por sus empleados y contratistas.

12.1. Responsabilidad Administrativa

a. La Dirección Técnica y el Área Tecnología Informática y Comunicaciones, deben garantizar la elaboración y actualización de un inventario de activos de información al mayor detalle posible, que garantice un fácil nivel de acceso, recuperación, trazabilidad, auditabilidad y responsabilidad de sus activos de información.

b. Se deben destinar las herramientas necesarias que permitan la oportuna gestión de inventarios de los activos de información, empleando como mínimo etiquetas de identificación externa, contemplando la posibilidad de tecnologías de captura de códigos de barras que faciliten la gestión de inventarios y el control de entradas y salidas de activos de las instalaciones de la organización.

12.2. Responsabilidad del usuario

a. Cada usuario es responsable del cuidado y uso adecuado de los recursos informáticos que se le asignen para el desarrollo normal de sus funciones.

b. Los recursos informáticos asignados a cada usuario, son para uso limitado para el desarrollo de sus funciones o actividades, por lo tanto, no está permitido el uso de cualquiera de los recursos con propósitos de ocio o lucro.

c. Los usuarios de los activos de información no podrán hacer uso de los elementos de cómputo asignados para realizar actividades personales distintas a las contratadas.

d. Los usuarios de activos de información son responsables ante la AGENCIA APP, de la protección de la información y los recursos asignados, por lo cual deben ser responsables de notificar al Área Tecnología Informática y Comunicaciones, la definición de controles de acceso y otros controles de seguridad, con el fin de garantizar su responsabilidad por incumplimientos, no conformidades y otros incidentes que se presenten en la AGENCIA APP.

e. La instalación de software no autorizado es responsabilidad del usuario, y cualquier daño en la configuración del equipo que se produzca por el incumplimiento de esta política debe ser asumido por el responsable del activo.

12.3. Gestión de activos

a. Todo cambio a la configuración de los computadores puede efectuarse únicamente por personal autorizado, y supervisión del Área Tecnología Informática y Comunicaciones.

b. Todos los activos de información (computadores, periféricos) deben estar protegidos por reguladores de voltajes y sus instalaciones eléctricas deben haber sido realizadas técnicamente controlando las fases correspondientes.

c. Todos los equipos de cómputo (servidores) y comunicaciones deben estar protegidos y soportados por equipos interrumpidos de poder UPS y sus instalaciones eléctricas deben haber sido realizadas técnicamente controlando las fases correspondientes. Cuando se concentren varios equipos en un área se debe hacer un estudio del consumo por equipo para determinar que el circuito no presente sobrecarga.

d. Todo el sistema eléctrico de cableado estructurado, debe estar independiente al sistema de energía de iluminación, y su gestión debe estar centralizada, acogiendo las normas eléctricas correspondientes para tal fin.

e. La única dependencia de la entidad con la potestad para tener acceso a la información y activos utilizados por los usuarios sin previa autorización, será la Dirección General y Dirección Técnica previo acompañamiento y asesoría por parte del Área Tecnología Informática y Comunicaciones.

f. La responsabilidad de la gestión de la seguridad de la información, la aplicación de reglas de controles de acceso definidas por los propietarios de los activos de información, estará a cargo del Área Tecnología Informática y Comunicaciones

12.4. Restricciones

a. No está permitida la descarga, instalación, almacenamiento y/o transferencia de juegos, archivos de audio, archivos de video, software y/o programas desde o hacia Internet, que atenten contra las leyes de derechos de autor, salvo los requeridos para el funcionamiento y mantenimiento de la plataforma tecnológica, gestionados por el Área Tecnología Informática y Comunicaciones.

b. Los activos de información no deben moverse o reubicarse sin la aprobación previa del Área involucrada. El traslado debe realizarlo únicamente el personal del Área Tecnología Informática y Comunicaciones, en caso de requerirse se deberá solicitar mediante el formato de Solicitud de Mantenimiento.

c. No está permitido el uso de hardware y/o softwares personales en las instalaciones de la AGENCIA APP, sin previa autorización de la Dirección Técnica y notificación al Área Tecnología Informática y Comunicaciones

d. No está permitido a los usuarios y/o visitantes: comer, fumar o beber en los puestos de trabajo, o instalaciones con equipos tecnológicos, sin excepciones; al hacerlo estarían exponiendo los equipos a daños eléctricos y a riesgos de contaminación sobre los dispositivos de almacenamiento.

e. Ningún ente interno o externo estará autorizado para generar copias de la información de la AGENCIA APP, sin previo aval por parte de la Dirección Técnica y/o el Área Tecnología Informática y Comunicaciones.

f. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

g. Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

12.5. Hardware

Objetivo: Establecer estándares para la configuración y mantenimiento de los Servidores de tal forma que se preserve la seguridad de los mismos, del software y datos en ellos instalado.

Configuración

a. El Área Tecnología Informática y Comunicaciones, debe implementar los protocolos y/o guías de configuración de todos los servidores de la AGENCIA APP, deben ser establecidas y actualizadas por cada tipo de Servidor.

b. Se debe tener toda la información de configuración por cada servidor, que garantice como mínimo: función principal, configuración de Hardware, configuración de Software, inventario de aplicaciones, servicios y servidores, ubicación de las copias de respaldo.

c. Debe existir el diagrama de configuración de plataforma y servidores.

d. La configuración de los servidores se debe hacer de acuerdo a los protocolos y/ guías establecidas por el Área Tecnología Informática y Comunicaciones.

Control de Accesos

a. Para la parametrización de los accesos privilegiados al servidor, la clave máster de "administrador" será gestionada únicamente por el responsable del Área Tecnología Informática y Comunicaciones, y debe existir una copia de respaldo compartida de la misma en poder de la Dirección Técnica.

b. La gestión de servidores se debe realizar únicamente bajo la utilización de canales seguros.

c. El acceso físico a servidores debe ser gestionado, programado y autorizado por el Área Tecnología Informática y Comunicaciones.

Gestión

a. La gestión, operación, instalación, desinstalación y mantenimiento de servidores es responsabilidad del Área Tecnología Informática y Comunicaciones, en la eventualidad de ser necesario contratar personal externo debe estar bajo supervisión.
b. El personal Informático externo debe ser altamente calificado en la gestión de servidores y notificar todas las novedades inherentes a la gestión del mismo.
c. La operación de servidores desde áreas de trabajo diferentes a las designadas para soporte técnico, debe ser autorizada por el Área Tecnología Informática y Comunicaciones.
d. Los cambios en la configuración de los servidores deben hacerse siguiendo los procedimientos establecidos para dicha operación.

Monitoreo

a. Para todos los eventos críticos de seguridad y los sistemas sensibles es necesario mantener registros y se deben gestionar acorde a lo establecido en los protocolos establecidos por el Área Tecnología Informática y Comunicaciones.
b. Todos los servidores deben tener activos los servicios de auditoría de eventos que garanticen la auditabilidad de las transacciones realizadas en ellos.
c. Todos los eventos relacionados con la seguridad, rendimiento, fallas y vulnerabilidades se deben reportar al Área Tecnología Informática y Comunicaciones, estos eventos se contemplan en los protocolos establecidos.
d. Debe existir un protocolo de acceso remoto, que garantice el adecuado uso de las herramientas existentes para tal fin.

Accesos Remotos

a. Toda herramienta de acceso remoto a servidores y equipos de cómputo, debe ser autorizada por el Área Tecnología Informática y Comunicaciones e instalada por el personal designado.

b. El acceso remoto a los equipos de cómputo será autorizado por el Área Tecnología Informática y Comunicaciones, previa solicitud por parte del responsable de cada Área, garantizando la confidencialidad de la información de cada usuario.

c. Los soportes remotos se realizarán únicamente en caso de no tener acceso directo al equipo que requiera el soporte, por eventos de localización física externa o distante de la AGENCIA APP.

d. Los accesos desde Internet para utilizar sistemas de información de la AGENCIA APP en forma remota y en tiempo real deben ser autorizados por el Área Tecnología Informática y Comunicaciones.

e. Todo acceso remoto debe ser establecido sobre Redes Privadas Virtuales - VPN con encriptación, previa configuración y aprobación por parte del Área Tecnología Informática y Comunicaciones.

f. Los accesos remotos para soportes en redes por terceros, proveedores de Servicios, deben ser asignados, aprobados y documentados por el Área Tecnología Informática y Comunicaciones.

g. La asignación de claves a terceros, proveedores de servicio, para la comunicación remota con la red central, debe estar supervisada permanentemente y será de asignación temporal.

12.6. Mantenimiento Equipos Servidores.

a. Se debe hacer el mantenimiento periódico del servidor, equipos de cómputo, utilizando el protocolo y/o procedimiento diseñado por el Área Tecnología Informática y Comunicaciones y será documentado acorde a los procedimientos establecidos.

b. Los procedimientos de instalación y mantenimiento de los servidores y equipos de cómputo deben ser actualizados con cada cambio de versión de los sistemas y aplicaciones por cada servidor.

c. Los parches más recientes de seguridad se deben probar, aprobar e instalar tanto al sistema operativo del servidor, como a las aplicaciones activas, a menos que esta actividad interfiera con la producción.

d. Los servicios, servidores y aplicaciones que no se utilicen, deben ser deshabilitadas y/o desinstaladas.

e. Debe mantenerse un inventario actualizado de software y hardware de cada uno de los servidores y computadores de la AGENCIA APP.

f. El Área de Tecnología Informática y Comunicaciones, debe generar los procedimientos y protocolos necesarios que garanticen la adecuada generación, custodia y disposición de las copias

de seguridad para los servidores de la AGENCIA APP, acordes con la política de Copias de Respaldo.

12.7. Gestión de Equipos de Cómputo

Objetivo: Establecer estándares para la configuración y mantenimiento de los Equipos de Cómputo y periféricos de tal forma que se preserve la seguridad de los mismos, del software y datos en ellos instalados.

Las políticas se aplican para el personal responsable de los equipos de cómputo y periféricos y a todos los usuarios de la AGENCIA APP, que tengan asignados recursos informáticos.

Configuración

a. El Área Tecnología Informática y Comunicaciones debe implementar los protocolos y/o guías de configuración de todos los equipos de cómputo y periféricos de la AGENCIA APP, deben ser establecidas y actualizadas por cada tipo de dispositivo.

b. Se debe tener toda la información de configuración por cada equipo de cómputo y periférico, que garantice como mínimo: función principal, configuración de Hardware, configuración de Software, inventario de aplicaciones, servicios, responsables.

c. La configuración de los equipos de cómputo y periféricos se debe hacer de acuerdo a los protocolos y/ guías establecidas por el Área Tecnología Informática y Comunicaciones.

d. Los equipos de cómputo y periféricos deben ser configurados de tal forma que los usuarios no puedan alterar la configuración ni instalar software.

Control de Accesos

a. Para la parametrización de los accesos a los equipos y periféricos, la clave será gestionada únicamente por el responsable del Área Tecnología Informática y Comunicaciones y debe ser estándar unificado para todos los equipos de la entidad.
b. Para la gestión de los equipos de cómputo y periféricos por parte del tercero Informático, se debe crear y asignar una clave con privilegios de administración, que será responsabilidad del personal asignado por el proveedor.
c. La correcta utilización de la cuenta de usuario para administración y su contraseña a nivel de computadores personales está bajo la responsabilidad del personal designado por el tercero Informático.

Gestión

a. La gestión, operación, instalación, desinstalación y mantenimiento de los equipos de cómputo y periféricos es responsabilidad del Área Tecnología Informática y Comunicaciones, en la eventualidad de ser necesario contratar personal externo debe estar bajo supervisión.

b. El personal informático externo debe ser calificado en la gestión de equipos y periféricos y notificar todas las novedades inherentes a la gestión del mismo.

c. Toda actividad que implique reasignación y traslado de equipos de cómputo y periféricos entre diferentes áreas de trabajo deben ser realizadas únicamente por el personal de sistemas o TI y autorizadas por la Dirección Técnica.

d. Los cambios en los equipos de cómputo y periféricos deben hacerse siguiendo los procedimientos establecidos para dicha operación.

Monitoreo

a. Para todos los eventos críticos de seguridad y los sistemas sensibles es necesario mantener registros y se deben gestionar acorde a lo establecido en los protocolos establecidos por el Área Tecnología Informática y Comunicaciones.

b. Todos los eventos relacionados con la seguridad, rendimiento, fallas y vulnerabilidades se deben reportar al Área de Tecnología Informática y Comunicaciones, estos eventos se contemplan en los protocolos establecidos.

c. Se deben garantizar los mecanismos necesarios que mitiguen el riesgo de extracción no autorizada de la AGENCIA APP, de equipos de cómputo y periféricos.

Mantenimiento Equipos de Cómputo.

a. Se debe hacer el mantenimiento periódico de los equipos de cómputo y periféricos, utilizando el protocolo y/o procedimiento diseñado por el Área Tecnología Informática y Comunicaciones, y será documentado acorde a los procedimientos establecidos.

b. Los procedimientos de instalación y mantenimiento de los equipos de cómputo y periféricos deben ser actualizados con cada cambio de versión de los sistemas y aplicaciones por cada equipo de cómputo o periférico.

c. Los parches más recientes de seguridad se deben probar, aprobar e instalar tanto al sistema operativo de equipos de cómputo y periféricos como a las aplicaciones activas, a menos que esta actividad interfiera con la producción.

d. Los servicios y aplicaciones que no se utilicen, deben ser deshabilitadas y/o desinstaladas.

e. Debe mantenerse un inventario actualizado de software y hardware de cada uno de los equipos de cómputo y periféricos de la AGENCIA APP.

f. El tercero Informático tiene la potestad para remover y notificar, cualquier software que no esté autorizado por el Área Tecnología Informática y Comunicaciones.

g. El Área Tecnología Informática y Comunicaciones debe generar los procedimientos y protocolos necesarios que garanticen la adecuada generación, custodia y disposición de las copias de seguridad para los Equipos de Cómputo y dispositivos de almacenamiento portátiles de la AGENCIA APP, acordes con la política de Copias de Seguridad.

Restricciones

a. Todos los usuarios de los equipos de cómputo y periféricos deben tener en cuenta los siguientes aspectos:

- No ingerir bebidas y/o alimentos cerca de los equipos de cómputo y periféricos
- No fumar dentro de las instalaciones y/o cerca a los equipos de cómputo y periféricos.
- No insertar objetos extraños en las ranuras de los equipos de cómputo y periféricos.
- No realizar actividades de mantenimiento de hardware
- No Instalar Software no autorizado en los equipos de cómputo y periféricos, si se instala software no licenciado, el usuario debe asumir las consecuencias legales y económicas.
- Apagar los equipos cuando no estén en uso.
- Bloquear la sesión cuando esté ausente.

b. Es responsabilidad del Área Tecnología Informática y Comunicaciones:

- Conservar los equipos en adecuadas condiciones ambientales
- Mantener una adecuada protección contra fluctuaciones de voltaje
- Todos los equipos de cómputo mantengan activa la política de equipos desatendidos.
- Únicamente el personal encargado puede instalar software en los equipos de cómputo y periféricos.
- Establecer programas de mantenimiento de equipos de cómputo y periféricos.

12.8. SOFTWARE

Gestión de Licenciamiento en Software Corporativo

Objetivo: Establecer estándares para la gestión de todo el Software empleado en la entidad.

Licenciamiento

a. Todo software corporativo, es decir sistemas operativos, sistemas de información y herramientas corporativas de gestión, debe ser direccionado, controlado de forma centralizada y gestionado operativamente en el Área de Tecnología Informática y Comunicaciones.

b. Todo software no comercial, es decir Freeware, Shareware, Trial, CPL, EPL, GNU, Open Source, debe tener el respectivo soporte de licencia, en el que se garantice el alcance de la licencia, y debe ser autorizado y gestionado por el Área de Tecnología Informática y Comunicaciones.

c. El Área de Tecnología Informática y Comunicaciones, será la única autorizada para realizar la instalación, configuración, parametrización, actualización y desinstalación.

d. Debe existir un inventario de las licencias de software de la organización, con el fin de facilitar la administración y control de software no licenciado.

Gestión

a. El Área de Tecnología Informática y Comunicaciones, debe garantizar la generación y actualización de inventarios de licenciamiento corporativo que garanticen la legalidad del mismo ante entes de control.

b. La utilización de software corporativo para fines personales, dentro o fuera de la entidad será responsabilidad de usuario del activo.

c. La extracción, préstamo, copia, venta y/o renta de software corporativo para fines externos y/o personales, no está autorizado bajo ninguna circunstancia.

Gestión de Vulnerabilidad

Objetivo: Reglamentar los controles necesarios para la prevención, detección y eliminación de virus informáticos en los equipos de cómputo de la AGENCIA APP.

Seguridad

a. Debe tener Software Antivirus que garantice la protección ante amenazas por virus informáticos, que a su vez debe contemplar como mínimo los siguientes componentes:

   - Componente de consola de servidor: encargado de distribuir y actualizar las actualizaciones de antivirus en los equipos de cómputo de la red.
   - Componente de correo externo: encargado de filtrar el contenido y tráfico de correos entrantes y salientes.

b. Debe existir uno o varios softwares que gestionen la salida hacia internet y desde internet, filtrado de contenidos, filtrado de páginas y monitoreo de navegación.

c. A nivel perimetral se debe contar con software de seguridad que permita controlar el acceso de virus, troyanos, malware, spyware, phishing y spam.

d. El software de detección de virus y demás Software de Seguridad seleccionados por la AGENCIA APP, deben ser instalado en todos los servidores y equipos de cómputo, incluyendo computadores portátiles de la AGENCIA APP.

e. Para la utilización de medios electrónicos externos, de uso corporativo y/o personal, correos electrónicos y descarga de archivos, se debe realizar previamente el escaneo o vacunación.

f. Los usuarios deben conocer los procedimientos de detección y eliminación de virus informáticos, para lo cual el Área de Tecnología Informática y Comunicaciones, debe garantizar el entrenamiento necesario para el uso de las herramientas de seguridad existentes.

g. Es responsabilidad del Área de Tecnología Informática y Comunicaciones, que todos los equipos asignados estén libres de virus, y responsabilidad de los usuarios que la información gestionada en los activos asignados, y medio de almacenamiento sean filtrados con el Software Antivirus y demás software de seguridad instalados en cada uno de los equipos de la AGENCIA APP.

Gestión de herramientas

a. Debe existir un protocolo de gestión de aplicaciones de seguridad informática que contemple las actividades de instalación, configuración, parametrización, administración, mantenimiento y desinstalación.

b. Debe realizarse la evaluación de la relevancia y criticidad o urgencia de los parches a implementar.

c. La instalación, configuración, parametrización, administración, administración, mantenimiento y desinstalación del software antivirus existente, es responsabilidad del Área Tecnología Informática y Comunicaciones.

d. La actualización del antivirus debe ser gestionada de forma centralizada en el servidor de la aplicación y de forma automática en cada uno de los equipos de cómputo de la AGENCIA APP.

e. Las actualizaciones de nuevas versiones serán gestionadas únicamente por el personal designado por el Área de Tecnología Informática y Comunicaciones.

f. Debe realizarse una evaluación periódica, mínimo cada 1 años, de la gestión y desempeño de las herramientas de seguridad informática existentes, y de ser necesario, cambiar las soluciones por aquellas que generen mayores características y niveles de seguridad.

Notificación de incidentes

a. Debe existir un formato de gestión de incidentes que registre todo el seguimiento de los incidentes presentados hasta su solución.

b. Los usuarios de cada uno de los Sistemas de información son responsables de solicitar soporte informático en caso de encontrar situaciones sospechosas en los sistemas asignados o cualquier virus detectado en equipos de cómputo asignados.

c. Todos los registros de detección de virus y otras vulnerabilidades, serán revisados y analizados por el personal designado y notificación al Área de Tecnología Informática y Comunicaciones.

Tratamiento de vulnerabilidades

a. Para todas las configuraciones de los sistemas de seguridad, se debe contemplar una política de cuarentena, que garantice que las vulnerabilidades encontradas no se difundan por las redes a otros equipos, hasta que se realice un análisis y tratamiento por parte del Área de Tecnología Informática y Comunicaciones.

12.9. Gestión de Trazabilidad y Auditabilidad

Objetivo: Reglamentar las pistas de Auditoría con las que deben contar los Sistemas de Información de la AGENCIA APP.

Tipo de información

a. Debe realizarse un análisis de riesgos sobre la criticidad de la información gestionada por los Sistemas Operativos, Bases de Datos, Sistemas de Información Corporativos propia y tercera, que identifique y defina los datos a los que deben aplicar las pistas de auditoría.

b. Debe existir un protocolo de configuración, implementación, gestión, respaldo y recuperación de pistas de auditoría, registros transaccionales y/o registros auditables.

c. Todos los Sistemas Operativos, Bases de Datos, Sistemas de Información Corporativos propios y terceros, debe tener activa y habilitada las funciones de registros para todas las transacciones a que dé lugar.

d. Las pistas de auditoría deben ser contempladas como un archivo adicional a los de datos, que evidencie todas las actividades realizadas por los usuarios, conteniendo como mínimo: fecha, hora, usuario, tipo de operación realizada (modificación, inclusión y borrado de información), archivo o tabla en la que se realizó la operación, número del registro o id, para el caso de modificación de información, debe incluir los campos de valor anterior y nuevo valor.

Control de accesos

a. El acceso a las pistas de Auditoría debe ser de carácter restringido a los Usuarios, solo el Área de Tecnología Informática y Comunicaciones, debe tener acceso a ellas.

b. Todo Sistema operativo, Base de datos, Sistema de información corporativos propios y terceros, deben permitir imprimir las pistas de auditoría.

c. Debe garantizarse la restricción de modificación a las pistas de Auditoría para todos los Sistemas Operativos, Bases de Datos, Sistemas de Información Corporativos propios y terceros.

d. Todas las aplicaciones deben tener Pistas de Auditoria, exceptuando aquellas aplicaciones que no manejen información crítica (aquella información que pueda causar pérdidas al ser manipulada) para la AGENCIA APP.

13. SISTEMAS DE INFORMACIÓN

13.1. Gestión de Sistemas Operativos

Objetivo: Establecer estándares para la Información que debe ser gestionada por los sistemas operativos de la AGENCIA APP.

Gestión

a. Deben existir protocolos de instalación, configuración, parametrización, gestión y soporte, de usuarios, roles y perfiles, para todos los sistemas operativos de la organización.

b. Deben aplicarse políticas de gestión y control propias de los Sistemas Operativos de servidor, que den cumplimiento al numeral anterior.

c. La instalación, configuración y parametrización de todos los sistemas operativos de la entidad, debe ser responsabilidad del Área Tecnología Informática y Comunicaciones.

d. Debe existir una política centralizada, incluida en los protocolos de configuración de equipos, que estandarice en todos los equipos de cómputo, el particionamiento de discos duros en 2 unidades virtuales: sistema operativo, datos y Copias de Seguridad local.

e. Debe aplicarse una política centralizada de Escritorios limpios que minimicen el riesgo de pérdida y confidencialidad de archivos, teniendo en cuenta que lo contenido en el escritorio es susceptible de pérdidas en caso de fallas del sistema operativo.

f. Debe aplicarse una política centralizada de Equipos desatendidos que garanticen confidencial de la información, cuando el usuario no esté en su puesto de trabajo.

g. El Área de Tecnología Informática y Comunicaciones, debe asignar a cada usuario 4 cuentas:

- Acceso a equipos de cómputo y red,
- Correo electrónico,
- Sistemas de Información corporativos y
- Herramientas de colaboración.

Seguridad

a. Debe existir un protocolo de encriptación de Información en los Sistemas Operativos y Redes.

b. Se deben habilitar todas las funcionalidades de los Sistemas Operativos de Servidor, de tal forma que toda la información viaje por las redes (LAN o WAN) en forma encriptada, con el fin de preservar su confidencialidad.

c. La encriptación de datos se debe realizar mediante Software y/o Hardware.

d. Todo tipo de información transmitida desde y hacia entidades externas, debe ser encriptado empleando las herramientas existentes para tal fin.

Directorio Activo

a. Debe existir un procedimiento de creación y eliminación de cuentas de usuario para Redes y Sistemas Operativos.

b. Se debe asignar una cuenta a todo usuario, que lo identificará al interior de la misma y les dará acceso a los recursos informáticos asignados.

c. Es responsabilidad del usuario, el buen uso y las actividades realizadas con la cuenta asignada.

d. La asignación de cuentas y configuración de perfiles debe ser solicitada por cada Área, y aprobada por la Dirección Técnica de la AGENCIA APP, una vez aprobada el Área de Tecnología Informática y Comunicaciones, crea las cuentas y perfiles en los sistemas a que dé lugar.

e. La estructura de creación de usuarios debe ser estandarizada y unificada para todos los sistemas operativos, bases de datos y sistemas de información internos y externos, y debe estar contemplada en el protocolo de creación de cuentas de usuario.

f. La cuenta de usuario de red del Administrador de la Red y su contraseña, debe ser conocida sólo por este, en caso de que otro usuario requiera realizar funciones propias del Administrador de la Red, por autorización expresa de éste, debe utilizar una cuenta alterna que contenga exclusivamente los permisos para realizar las actividades para la cual está autorizado.

g. Las claves deben ser cambiadas en forma forzosa por lo menos 3 vez cada año.

Responsabilidades

a. Las cuentas de usuario de la red corporativa son personales e intransferibles. Bajo ninguna circunstancia este tipo de cuentas deben ser conocidas por una persona diferente a su propietario.

b. Toda novedad presentada en la planta de personal de los empleados y contratistas de la AGENCIA APP, (ingresos, licencias, sanciones, suspensiones, ascensos y/o retiros) debe ser reportada al Área Tecnología Informática y Comunicaciones.

Control de Accesos

a. No se deben asignar cuentas de usuario genéricas, entendiendo como genérica aquellas que son utilizadas por varios usuarios de la entidad.

b. Todas las cuentas serán creadas con los permisos del grupo general, si el usuario necesita permisos adicionales o necesita pertenecer a un grupo específico para acceso a recursos propios de su trabajo debe hacer una solicitud sustentada al Área Tecnología Informática y Comunicaciones.

c. Las cuentas de usuario de la red deben ser suspendidas cada vez que un empleado y contratista de la AGENCIA APP, se ausente por largo tiempo por motivo de incapacidad, licencia, vacaciones, suspensión de contrato, entre otras. La cuenta sólo será habilitada durante este período de tiempo bajo solicitud escrita debidamente justificada por la Dirección Técnica.

d. Las características de asignación de claves, debe estar acorde a lo contemplado en el protocolo correspondiente.

Recomendaciones

a. NO se debe revelar información de cuentas ni contraseñas a NADIE, por ningún medio (teléfono, correo, o personalmente).

b. NO se deben escribir las claves en medios físicos (papel, agenda libreta, etc.)

c. NO se debe revelar, compartir, prestar o hablar de las claves, o formato de claves a nadie de la AGENCIA APP, incluyendo miembros de la Junta, ni a miembros de la familia, conocidos o amigos.

d. NO debe suministrar ni delegar las claves en periodos de ausencia, calamidad o vacaciones.

e. NO debe habilitarse en ningún sistema o aplicación, la característica de recordación de claves.
f. NO debe guardar claves en ningún tipo de computador sin utilizar un mecanismo de encriptación.

g. NO se deben utilizar las cuentas y claves asignadas en equipos externos a la AGENCIA APP, o que considera no confiable.

h. Las claves se deben crear de manera que puedan ser fácilmente recordadas.

i. Cualquier empleado y contratista que se encuentre responsable de violar esta política está sujeto a acciones disciplinarias correspondientes.

13.2. Gestión de Sistemas Propios

Objetivo: Definir las herramientas para hacer desarrollos (Base de Datos y Lenguaje de Programación), así como la forma para realizar los cambios y mantenimiento a dicho software.

Proyectos de desarrollo

Para todo desarrollo de Software en la AGENCIA APP, o para cumplimiento de proyectos especiales que involucren aplicaciones o sistemas de información, el Área de Tecnología Informática y Comunicaciones, debe diseñar los formatos necesarios para documentar las siguientes actividades:

- Un análisis de requerimientos internos, que debe ser revisado por el Área Tecnología Informática y Comunicaciones, y aprobado por la Dirección Técnica.
- Un documento RFI – Requerimiento de Información, para entregar al proveedor de la solución.
- Un análisis técnico de requerimientos, como respuesta por parte del proveedor de la solución.
- Un documento RFP - Requerimiento de Propuesta, para entregar al proveedor de la solución.
- Un documento propuesto, que debe contemplar: Análisis situacional, matriz de riesgos del proyecto, propuesta económica, propuesta técnica, documentación legal y jurídica, demás soportes requeridos acordes a cada proyecto.
- Todos los documentos anteriores deben presentarse a la Dirección General y Dirección Técnica.

Ciclo de vida de desarrollo de Software

Debe definirse y aplicarse una metodología de desarrollo de aplicativos que contemple como mínimo las siguientes fases:

- Concepción / análisis de negocio: Se debe exigir para todo desarrollo de Software, un levantamiento de información, un análisis situacional y deben estar claramente documentadas.
- Planeación y diseño: Debe contemplar un diseño de la solución y un plan de ejecución.
- Desarrollo: Debe especificar las herramientas de desarrollo, la estructura y arquitectura de la solución, modelo entidad-relación y diccionarios de datos.
- Prototipo y pruebas: Debe contemplar la presentación de prototipos de evaluación y ajuste.

- Instalación y estabilización: Debe contemplar plan de implementación, migración y estabilización de la solución.

- Soporte y mantenimiento: Debe contemplar el plan de mantenimientos correctivos, niveles de acuerdo de servicios y plan de continuidad de la solución que incluya plan de respaldo, plan de recuperación y plan de contingencia. Para cada solución se deben entregar: Manual de Usuario, Manual de administración, Manual Técnico de Instalación y configuración.

Ambientes de trabajo

a. Para la adecuada gestión de proyectos de desarrollo, mantenimientos, pruebas e implementaciones, el Área de Tecnología Informática y Comunicaciones, debe implementar la infraestructura mínima de seguridad que garantice la adecuada gestión y control de los proyectos de software, implementando con los recursos existentes de la AGENCIA APP, los siguientes ambientes tecnológicos:

- **Ambiente de desarrollo:** Configuración orientada a la generación de desarrollos, en el cual los desarrolladores crean y modifican los objetos a solicitud del área responsable de la Información.

- **Ambiente de Pruebas:** Configuración orientada a la generación de pruebas por parte del Área Tecnología Informática y Comunicaciones, y por el usuario, réplica del ambiente de producción en donde se realizarán todas las pruebas necesarias para garantizar el buen funcionamiento de los aplicativos.

- **Ambiente de Producción:** Configuración orientada al usuario final, ambiente donde se realiza el procesamiento real de la información utilizada para la toma de decisiones de AGENCIA APP.
  Para cada ambiente debe existir una configuración independiente en Sistema Operativo, Base de Datos y aplicación.

Plan de Pruebas

a. Debe existir un procedimiento de pruebas a programas que defina actividades y responsables.

b. Debe definirse un plan de pruebas que especifique escenarios de pruebas, niveles y tipos de pruebas que se deban realizar a los aplicativos.

c. Los datos del ambiente de pruebas deben ser una réplica del ambiente de producción.

d. El resultado de las pruebas debe documentarse por los desarrolladores en conjunto con los usuarios del área solicitante.

Control de cambios

a. El Área de Tecnología Informática y Comunicaciones, debe integrar y mantener todas las actividades de gestión de cambios (documentación y formación procedimental para usuarios y administradores) del Software / aplicaciones.

b. Debe disponerse de un inventario de aplicativos actualmente existentes en la AGENCIA APP, especificando si se encuentran en producción o desarrollo, si ha sido un desarrollo propio o adquisición a terceros.

c. Para todos los cambios y ajustes autorizados, y en ejecución se debe conservar un registro escrito de las modificaciones realizadas, para lo cual se debe crear un registro de control de cambio.

d. Los cambios de emergencia deben ser debidamente aprobados, auditados y documentados.

e. Todo cambio a los aplicativos debe ser solicitado por la Dirección Técnica. Si se requieren cambios a los datos, deben ser aprobados por el responsable de la información y se debe crear un formato de cambios de información.

f. Debe existir un procedimiento para la solicitud, autorización y aprobación para todos los cambios a los aplicativos.

g. La documentación de todas las aplicaciones de la AGENCIA APP, debe ser permanentemente actualizada por los desarrolladores.

Seguridad en desarrollos

a. El Área de Tecnología Informática y Comunicaciones, debe implementar los mecanismos y herramientas necesarias para garantizar la seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios del Software / aplicaciones, que se desarrollen interna o externamente, para la AGENCIA APP.

b. Todos los Sistemas de Información deben contar con usuario y clave (Fuerte) la clave debe estar encriptada.

c. Todos los Sistemas de Información deben permitir restringir el acceso a las opciones de la aplicación utilizando para ello, los perfiles de acceso.

d. Los perfiles de acceso deben ser de acceso restringido, tan solo el administrador del Sistema de Información debe tener acceso a los mismos.

e. Todas las aplicaciones deben tener pistas o registros de auditoría (al menos para los datos críticos), en el cual se pueda identificar quien ha realizado cambios, borrados o inserción de datos no autorizados.

f. Las pistas de auditoría no deben permitir cambios de las mismas (son únicamente de lectura).

Plataforma de desarrollos

a. Deben existir los mecanismos y herramientas necesarias que restrinjan el acceso a las bases de datos en las que se almacena la información institucional.

b. Debe existir una Base de Datos, con igual configuración y parametrización, por cada ambiente de trabajo.

c. Debe existir un Lenguaje de desarrollo, que garantice fácil integración con los demás sistemas de información de AGENCIA APP.

14. TERCEROS

Definir las responsabilidades y parámetros de gestión de los terceros.
Esta Política aplica a todos los terceros y/o contratistas involucrados con la AGENCIA APP.

14.1. GESTIÓN

a. Debe existir un proceso y procedimientos que determinen la selección y contratación de proveedores de servicios, bienes, muebles e inmuebles.

b. Debe existir un proceso y procedimientos que determinen las actividades de compra de servicios, bienes, muebles e inmuebles.

c. Debe existir un proceso y procedimientos que determinen los mecanismos de evaluación de la gestión de proveedores de la AGENCIA APP.

d. Deben existir ANS - Acuerdos de Nivel de Servicio con todos los proveedores de servicios y productos de Tecnologías de Información y Comunicaciones, que garanticen la confiabilidad, integridad y disponibilidad de los servicios y productos contratados.

e. Deben existir Acuerdos de Confidencialidad con todos los proveedores de Tecnologías de Información y Comunicación, o cláusulas de confidencialidad en los contratos establecidos, que garanticen la confidencialidad de la información de la AGENCIA APP.

f. Debe existir un proceso y procedimientos de seguimientos y controles a la gestión de proveedores de Servicios y productos de Tecnologías de información y Comunicaciones.

g. Deben existir mecanismos de evaluación de proveedores de servicios y productos, de forma periódica.

h. Deben existir mecanismos de valoración de los servicios y productos recibidos, periódicamente.

14.2. SERVICIOS

a. Se deben exigir a los proveedores de Tecnologías de Información y Comunicaciones, las certificaciones de implementación de buenas prácticas, estándares internacionales y/o modelos de madurez, tales como ISO-9001, ISO-27001, ISO-20000, CMMI o ITIL, acorde a la prestación de sus servicios.

b. Todo proveedor de Servicios de Tecnologías de Información y Comunicaciones, debe establecer un mecanismo adecuado que permita realizar la gestión de solicitudes, incidentes, eventos y problemas que se puedan presentar con sus respectivas soluciones.

14.3. RESPONSABILIDADES

Todo proveedor de Servicios de Tecnologías de Información y Comunicaciones es responsable por el buen uso y cuidado de todos y cada uno de los elementos y componentes de la infraestructura y plataforma tecnológica de la AGENCIA APP, a que tenga contacto, por la naturaleza de sus servicios y/o productos.

15. POLÍTICAS Y ESTANDARES DE REDES Y COMUNICACIONES

15.1. Gestión de Redes

Objetivo: Establecer estándares para proteger la integridad de información que es transmitida interna y externamente, contra amenazas y vulnerabilidades.

Gestión

a. Se debe contar con un procedimiento para la administración de todas las redes corporativas.

b. Debe existir un protocolo de configuración de todas las redes corporativas, relacionadas con el diseño de los sistemas de comunicación y cómputo de la AGENCIA APP.

c. Se debe realizar un monitoreo permanente tanto de la infraestructura de comunicaciones como de los servidores, de manera que se detecten los problemas que pueden llegar a causar fallas en la disponibilidad de los servicios de las redes de la AGENCIA APP.

d. Los centros de cableado, Centro de Servidores y Centros Eléctricos, están catalogados como zonas restringidas, con control de acceso y restricción a personal no autorizado.

Seguridad

a. Deben existir protocolos de parametrización y directrices de seguridad informática para redes y herramientas de seguridad de red como IDS-Sistemas de Detección de Intrusiones, IPS-Sistemas de Prevención de Intrusiones, gestión de vulnerabilidades, y demás a que dé lugar.

b. Deben existir protocolos de transmisión de información que garanticen que todos los datos que se transmitan por las redes internas de la AGENCIA APP, y entre redes externas, sean encriptados.

c. La configuración de accesos a la información de las estaciones de trabajo desde la red, deben tener acceso restringidos a los directorios que garanticen la restricción de accesos no autorizados.

d. La información enviada a las entidades externas (sean archivos o sea para alimentar una terminal que permita consultar o procesar información de la AGENCIA APP, debe viajar encriptada.

e. Debe existir un protocolo de monitores de seguridad en todas las redes que permita periódicamente la realización de monitoreo a los ataques en tiempo real, y garantice la seguridad de las redes ante terceros no autorizados e intrusos.

f. Deben existir protocolos de verificación física a las redes corporativas que garanticen la calidad de las instalaciones de cableado de datos

Controles de Acceso

a. Deben existir los protocolos de seguridad que describan los mecanismos de control y accesos a las diferentes redes existentes en la AGENCIA APP.

b. Deben existir todos los documentos técnicos que describan las configuraciones de red y su interacción con componentes internos y externos.

c. Deben existir los protocolos que describan controles de seguridad perimetrales de las Redes de Área Local – LAN y Redes de Área Global – WAN; e internos entre Redes de Área Local LAN y Redes de Área Local Wifi - WLAN; y su integración con los controles de seguridad en sistemas operativos de plataforma y aplicaciones corporativas.

d. La gestión de accesos, roles y perfiles de las redes corporativas deben estar contempladas y gestionadas desde la gestión del Directorio Activo de los sistemas operativos de plataforma tecnológica.

Restricciones

a. Los usuarios de la red interna de la AGENCIA APP, no pueden realizar o ejecutar acciones en la red que sean exclusivas de los administradores de red.

b. Los usuarios no deben llevar a cabo ningún tipo de instalación de líneas telefónicas, canales de transmisión de datos, módems, ni cambiar su configuración sin haber sido formalmente aprobados por el Área de Tecnología Informática y Comunicaciones.

15.2. Comunicaciones

Gestión de Internet

Objetivo: Garantizar el uso adecuado de Internet como herramienta fuente de información, investigación y comunicación en AGENCIA APP.

Gestión

a. El servicio de Internet debe ser utilizado para facilitar el cumplimiento de las funciones asignadas a los empleados y contratistas de AGENCIA APP.

b. Debe existir un protocolo de acceso a internet que garantice el buen uso de éste y de las herramientas disponibles para su gestión.

c. Toda conexión entre las redes corporativas y redes externas de servicios (Outsourcing), redes públicas e Internet, debe contar como mínimo con mecanismos de control de acceso lógico (validación y autenticación de usuarios).

d. Debe existir un proceso y procedimientos que garanticen el monitoreo y revisiones periódicas del uso apropiado de Internet.

Seguridad

a. Deben existir los mecanismos de gestión y control apropiados para garantizar el adecuado uso del internet tales como Firewall, Proxy, DNS, Filtro de Contenidos, Anti-virus, anti-spam, anti-spyware, anti-phising, anti-malware y demás software para gestión de vulnerabilidades de redes, aprobados por el Área de Tecnología Informática y Comunicaciones y avaladas por la Dirección Técnica.

b. Los usuarios con acceso a Internet deben estar seguros de los sitios visitados, identificando las advertencias de acceso a sitios desconocidos.

c. No se debe registrar en los sitios de Internet datos específicos de las máquinas de la AGENCIA APP, como la dirección IP, nombre de la máquina, nombres de usuarios, claves, nombre de redes corporativas entre otros, que puedan exponer la confidencialidad de las redes y exponerse a la recepción no deseada de mensajes o información.

Responsabilidades

a. El usuario es responsable por respetar y acatar las leyes para derechos de reproducción, patentes, marcas registradas y todo lo relacionado con derechos de autor las cuales aplican en Internet.

b. Para inscripciones y transacciones comerciales en Internet se debe entender que esta clase de actuaciones no compromete en forma alguna los recursos económicos de la AGENCIA APP, ni implica responsabilidad por parte de esta. En todo caso si se llega a presentar, se entiende que compromete exclusivamente al empleado y la Entidad podrá tomar las acciones del caso.

c. Se debe hacer uso racional del servicio de Internet, y se considera como uso indebido cuando:

- Atenta contra la integridad, veracidad y confidencialidad de la información de la AGENCIA APP.
- Atenta contra la integridad de los componentes de la plataforma tecnológica
- Reduce la productividad de los funcionarios y contratistas.
- Pone en riesgo la disponibilidad de los recursos informáticos de la AGENCIA APP.

Restricciones

a. Está prohibido el acceso a sitios de pornografía y de cualquier otra índole que atente contra la integridad de los funcionarios, contratistas de la AGENCIA APP y cualquier otra persona.

b. Los funcionarios y contratistas deben limitar su acceso a páginas de entretenimiento, distracción o correos en portales públicos. La AGENCIA APP, podrá aplicar restricciones o sanciones en casos que se encuentren excesos.

c. Se debe auto-regular el uso de herramientas de mensajería instantánea y chat, tales como WhatsApp, Skype, Messenger, Yahoo Messenger, Gmail Talk, entre otros, en horas laborales o cuestiones de trabajo, evitando que se afecte la productividad.

d. No está permitido instalar y usar juegos en los computadores, debido que estos se deben usar como una herramienta de trabajo y no como forma de distracción.

e. No está permitido descargar música de ningún sitio de Internet, entre otros: mp3, mp4, wav, wma, midi, mpeg, jpeg, jpg, gif, o cualquier otro formato existente, dado que ello constituye una violación al derecho de autor sobre ese tipo de obras grabadas.

f. No está permitido instalar software P2P – Per-to-Per en los computadores ya que este software afecta el rendimiento del canal corporativo de Internet y puede impactar la vulnerabilidad de las redes corporativas.

g. No está permitido descargar ni instalar software de Internet. El único personal autorizado para instalar cualquier tipo de software será el Área Tecnología Informática y Comunicaciones, acorde a las políticas existentes.

15.3. Gestión de Intranet

Objetivo: Garantizar el uso adecuado de Intranet como herramienta fuente de información, investigación y comunicación en AGENCIA APP,

Gestión

a. El servicio de Intranet debe ser utilizado para facilitar el cumplimiento de las funciones asignadas a los funcionarios y contratistas de la AGENCIA APP.

b. Debe existir un procedimiento de administración de la intranet, en especial el mantenimiento y depuración de la información publicada, que garantice el buen uso de este y de las herramientas disponibles para su gestión.

c. La información de Intranet debe ser únicamente utilizada por personal autorizado. Los usuarios no deben re-direccionar información que aparezca en Intranet a terceros sin autorización de la AGENCIA APP.

d. La información que se publique en la Intranet de la AGENCIA APP, debe contar con la aprobación del responsable de cada Área y bajo la coordinación del Área de Tecnología Informática y Comunicaciones, encargada de la administración de la página web, y la del propietario de la información involucrada

Seguridad

a. Deben existir los mecanismos de gestión y control apropiados para garantizar el adecuado uso de la Intranet, tales como Firewall, Proxy, DNS, Filtro de Contenidos, Anti-virus, anti spam, anti-spyware, anti-phising, anti-malware y demás software para gestión de vulnerabilidades de redes, aprobados por el Área Tecnología Informática y Comunicaciones, y avaladas por la AGENCIA APP.

b. El material que se publique en la Intranet de la AGENCIA APP debe ser revisado previamente para confirmar la actualidad, oportunidad e importancia de la información y evitar que los programas o archivos incluyan virus. Así mismo, se debe evaluar posibles problemas operativos y de seguridad de acuerdo con las políticas establecidas.

Responsabilidades

Se debe hacer uso racional del servicio de Intranet, y se considera como uso indebido cuando:

- Atenta contra la integridad, veracidad y confidencialidad de la información de la AGENCIA APP.
- Atenta contra la integridad de los componentes de la plataforma tecnológica.
- Reduce la productividad de los empleados y contratistas.
- Pone en riesgo la disponibilidad de los recursos informáticos de la AGENCIA APP.

Restricciones

a. Está prohibida la publicación de material de pornografía y de cualquier otra índole que atente contra la integridad de los usuarios de la entidad y cualquier otra persona.
b. No está permitido publicar o usar juegos en redes internas de trabajo.
c. No está permitido publicar, transmitir, almacenar o copiar música desde ni hacia componentes de redes, unidades publicar o unidades internas de la organización.
d. No está permitido publicar, transmitir, almacenar o copiar software corporativo u otros.

15.4. Gestión de Correo Electrónico

Objetivo: Evitar la propagación de correo basura, o cualquier tipo de virus a través del correo interno de la entidad, prevenir o proyectar una mala imagen pública de la AGENCIA APP, cuando se utilice el correo.

Gestión

a. Debe existir un protocolo de gestión y asignación de correos electrónicos.

b. Todos los empleados y contratistas de la AGENCIA APP, tendrán correo electrónico personalizado el cual se implementará en la medida en que se disponga de computadores para tal fin.

c. Todas las direcciones de correo electrónico deben ser creadas usando el estándar establecido por la AGENCIA APP, y deben tener una cuota de almacenamiento máximo.

d. El correo de la AGENCIA APP, no se debe usar para la creación o distribución de cualquier mensaje corrupto u ofensivo, incluyendo comentarios ofensivos acerca de raza, genero, color del cabello, discapacidades, edad, orientación sexual, pornografía, creencias o prácticas religiosas, creencias políticas o nacionalidad. Cualquier empleado y contratista que reciba mensajes de correo con este tipo de contenido desde cualquier cuenta de la AGENCIA APP, debe reportar este asunto al Área de Tecnología Informática y Comunicaciones.

e. Se debe eliminar todo el correo basura cartas cadena o similares inmediatamente sin reenviarlo. Los empleados y contratistas de la AGENCIA APP, no deben contar con ningún tipo de privacidad respecto de cualquier información que guarden, envíen o reciban en el sistema de correo de la AGENCIA APP.

f. Usar una cantidad razonable de los recursos de la AGENCIA APP, para mensajes de correo personales es aceptable. Los mensajes de correo que no sean relacionados con el trabajo se deben guardar en una carpeta separada de los mensajes de oficina.

Seguridad

a. Está restringido el envío y recepción de archivos comprimidos en formato Zip o Rar, dados los riesgos asociados a los mensajes provenientes de entes externos o fuentes no confiables con fines malignos. Para el Área de Tecnología Informática y Comunicaciones, se contempla excepción controlada por la naturaleza de la información que transmite con diversos entes asociados.

b. Debe existir una herramienta o mecanismo de encriptación establecido como estándar, para los mensajes de correo intercambiados con entes externos.

c. Se debe realizar un análisis de virus, con la herramienta asignada para tal fin, de todos los archivos adjuntos que son enviados o recibidos por el correo electrónico.

d. Todo incidente de seguridad o desempeño del correo electrónico, debe ser notificado al Área de Tecnología Informática y Comunicaciones, empleando los canales establecidos para tal fin.

Responsabilidades

a. El usuario responsable del buzón debe dar un trámite ágil al correo electrónico recibido (responder, eliminar, archivar mensajes en el disco duro local).

b. El sistema de correo electrónico debe ser utilizado únicamente para la transmisión de información relacionada con asuntos laborales o de prestación de servicio del usuario y/o asuntos de interés común que incidan en la buena marcha y en el mejoramiento de la armonía laboral de la AGENCIA APP.

c. Los buzones de correo configurados son de uso exclusivo del usuario al que fue asignado y serán de su responsabilidad todos aquellos mensajes enviados en su nombre.

d. Es responsabilidad de los usuarios de correo electrónico mantener o archivar los mensajes enviados y/o recibidos para efectos de soportar ante terceros (internos o externos) la ejecución de operaciones o acciones.

e. Es responsabilidad de los usuarios de Correo Electrónico hacer limpieza / depuración a su buzón de correo.

f. Todos los mensajes que se envíen a través del correo electrónico deben estar enmarcados en normas mínimas de respeto.

g. El mantenimiento de la lista de contactos y del buzón de correo será responsabilidad del usuario del servicio conservando únicamente los mensajes necesarios, con el fin de no exceder el máximo tope de almacenamiento.

Restricciones

a. Está prohibido enviar cartas, cadenas o mensajes con bromas desde un correo de la AGENCIA APP, así como enviar alertas o correos masivos a menos que se tenga autorización del Área de Tecnología Informática y Comunicaciones.

b. Los usuarios de correo electrónico de la AGENCIA APP, no deben generar mensajes para dar trámite de operaciones o actividades propias de la AGENCIA APP, en herramientas de software diferentes a las versiones autorizadas, adquiridas e instaladas por el Área de Tecnología Informática y Comunicaciones,

se deja excepción para personal que no se encuentre en la AGENCIA APP, por la naturaleza de sus funciones o actividades.

c. El correo electrónico no debe ser utilizado por terceros (clientes o proveedores) sin previa autorización.

d. No está permitido la parametrización de los mensajes a enviar, que contengan fondos, imágenes o logos no corporativos.

e. Los usuarios de la AGENCIA APP, no deben utilizar versiones escaneadas de firmas hechas a mano para dar la impresión de que un mensaje de correo electrónico o cualquier otro tipo de comunicación electrónica ha sido firmada por la persona que la envía.

f. No se debe abrir o revisar correo que tenga procedencia de remitentes desconocidos.

g. Como uso inapropiado del correo electrónico se considera:

I. Intentos de acceso y/o accesos no autorizados a otra cuenta de correo.
II. Transmisión de mensajes de correo con información sensible o confidencial a personas u organizaciones externas sin autorización.
III. Cadenas de mensajes que congestionen la red.
IV. Transmisión de mensajes obscenos.
V. Cualquier actividad no ética que afecte a la AGENCIA APP.
VI. Enviar correo a nombre de otra persona.
VII. Prestar el buzón de Correo a personas diferentes a las asignadas por la AGENCIA APP.

16. POLITICAS Y ESTANDARES DE SEGURIDAD DE CONTINUIDAD DE NEGOCIO

16.1. Copias de Seguridad

Gestión de Copias de Seguridad

Objetivo: Garantizar que toda la información almacenada en los componentes de la plataforma tecnológica de la AGENCIA APP, se encuentre debidamente respaldada mitigando el riesgo de pérdida de la información.

Gestión

a. Debe existir un procedimiento que determine actividades, periodicidad, responsables y mecanismos de almacenamiento de las copias de respaldo de todos los sistemas de información de la AGENCIA APP.

b. Debe existir una definición formal de las políticas y procedimientos de generación, retención y rotación de copias de respaldo.

c. Debe existir un Plan de Copias de Respaldo, y debe contemplar la generación de copias de respaldo de los sistemas operativos, los sistemas de información, las aplicaciones corporativas, acorde con los procedimientos establecidos en el Plan de contingencia y en los procedimientos diseñados para realizar dicha actividad.

d. Cada vez que se cambien los servidores o el Software, los procedimientos para realizar las Copias de Respaldo y el Plan de Contingencia deben ser actualizados.

e. Con el objetivo de garantizar la continuidad del servicio, se determina como de carácter obligatorio, la ejecución de políticas y procedimientos relacionados con copias de respaldo definidas por la AGENCIA APP.

Generación

a. La generación de las Copias de Respaldo se debe realizar con base en el resultado de los análisis de riesgos de la información existente y vigente en la entidad.

b. Debe existir un protocolo de generación de Copias de Respaldo por cada sistema operativo, sistema de información y aplicación corporativa, que contemple la definición de los tipos de copias, tipos y medios de almacenamiento, aplicación de respaldo, frecuencia de copia, plan de prueba, esquemas de seguridad y actividades de restauración.

c. Cada vez que se cambien los servidores o el Software, los procedimientos para realizar el Copias de Respaldo y el Plan de Contingencia deben ser actualizados.

d. Se deben realizar prueba de los medios utilizados con el fin de asegurar su adecuado funcionamiento o descartarlos.

Almacenamiento y custodia

a. Deben usarse medios que permitan almacenar la información apropiadamente, no utilizar CD o DVD ya que dichos medios se degradan y la información se pierde.

b. Los medios deben ser almacenados en un sitio que posea las condiciones ambientales correctas (Temperatura y Humedad), el cual asegure el adecuado funcionamiento de los mismos.

c. Los medios deben contar con un periodo de vida (registro de fecha de inicio del uso de los mismos y una fecha de descarte).

d. Los medios descartados no se deben usar ya que existe el riesgo de pérdida de la información en ellos almacenada.

e. Todos los medios se deben mantener en un área restringida y bajo llave.

f. El acceso a los medios será autorizado únicamente al Área de Tecnología Informática y Comunicaciones, o al personal que sea autorizado por dicha área.

g. Los medios deben estar adecuadamente etiquetados de tal forma que sean fácilmente identificables.

h. El contrato de los medios almacenados en instalaciones externas, debe contar con una cláusula de Confidencialidad la cual asegure que la información no pueda ser copiada o divulgada en forma no autorizada.

i. Se debe tener un registro de los medios enviados a sitio externo, firmado por el tercero que reciba dichos medios o su representante.

Responsabilidades

a. La gestión y ejecución de las copias de respaldo es responsabilidad del Área de Tecnología Informática y Comunicaciones.
b. La responsabilidad de verificar la realización de copias de respaldo de los servidores y de las estaciones de trabajo es del Área Tecnología Informática y Comunicaciones.

c. El almacenamiento de las copias de respaldo es responsabilidad del Área Tecnología Informática y Comunicaciones.

d. El Área Tecnología Informática y Comunicaciones, debe garantizar la realización de las copias de respaldo acorde a la frecuencia y alcance identificados en el Análisis de Riesgos de la información.

Seguridad

a. Todas las copias de respaldo deben estar encriptadas.

b. El acceso al registro de ubicación y contenido de los medios debe estar restringido.

c. Se debe contar con un registro, el cual permita identificar la ubicación (centro externo o cinto teca) y el contenido de cada medio (con un número o un código)

16.2. Contingencia Y Recuperación De Desastres

Gestión de Contingencias

Objetivo: Regular las actividades a realizar ante situaciones de contingencia.

Alcance: Esta Política cubre todas las situaciones de contingencia que se pueden presentar, tales como: incendios, terremotos, inundaciones, tanto en la oficina principal, como en los diferentes sitios donde se resguardan equipos informáticos en todas las instalaciones de la AGENCIA APP, pertenezcan o no al mismo.

Gestión

a. Debe existir un BCP-Plan de Continuidad de Negocio, que a su vez involucre un Análisis de Riesgos, Plan de Contingencias, Plan de Recuperación de Desastres y Plan de Disponibilidad, con el objetivo de garantizar la continuidad en el funcionamiento de los activos tecnológicos de AGENCIA APP, y es responsabilidad de su elaboración el Área de Tecnología Informática y Comunicaciones, y de su aprobación la Dirección Técnica.

b. Debe existir un protocolo de acción y un cronograma de ejecución, pruebas y ajustes, por cada uno de los planes enunciados anteriormente.

c. Se entiende por Plan de Continuidad de Negocio todas las acciones administrativas y/o operacionales tendientes a garantizar la continuidad del negocio ante eventualidades externas o internas que atente contra el normal funcionamiento de la organización.

d. Se entiende por Análisis de Riesgos el estudio que se realiza por un ente interno y/o un ente externo, con el objetivo de identificar los riesgos existentes, la probabilidad de ocurrencia y su impacto, para finalmente determinar los controles que mitiguen los riesgos identificados.

e. Se entiende por Plan de Contingencia todas las acciones administrativas y/o operacionales tendientes a superar fallas, incidentes y eventos en general que interrumpan el normal funcionamiento de los activos tecnológicos de la AGENCIA APP.

f. Se entiende por Plan de Recuperación de Desastres todas las acciones administrativas y/o operacionales tendientes a restaurar todos los componentes afectados una vez se han presentado pérdidas materiales o físicas en eventos o situaciones catastróficas.

g. El plan de Contingencias debe permitir reaccionar ante eventos no esperados sea por efectos de la naturaleza o humanos (robo, sabotaje, terremoto, incendio, inundación, toma de las instalaciones de la AGENCIA APP, entre otros).

h. El Área de Tecnología Informática y Comunicaciones, es responsable de establecer períodos de actualización, mantenimiento y pruebas del Plan de Continuidad del Negocio.

17. DEFINICIONES

Acceso físico: La posibilidad de acceder físicamente a un computador o dispositivos, manipularlo tanto interna como externamente.

Acceso lógico: Ingresar al sistema operativo o aplicaciones de los equipos y operarlos, ya sea directamente, a través de la red de datos interna o de Internet.

Activos de Información: Toda aquella información que la Entidad considera importante o fundamental para sus procesos, puede ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, software del sistema, etc.

Amenaza: Es la causa potencial de un daño a un activo de información.

Aplicaciones o aplicativos: Son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares.

Cableado estructurado: Cableado de un edificio o una serie de edificios que permite interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía, control, etc.

Cifrado de datos: Proceso por el que una información legible se transforma mediante un algoritmo (llamado cifra) en información ilegible, llamada criptograma o secreto. Esta información ilegible se puede enviar a un destinatario con muchos menos riesgos de ser leída por terceras partes.

Confidencialidad Se debe entender como la característica de prevenir la circulación de información a personas, entes o sistemas no autorizados.

Configuración Lógica: Conjunto de datos que determina el valor de algunas variables de un programa o de un sistema operativo, elegir entre distintas opciones con el fin de obtener un programa o sistema informático personalizado o para poder ejecutar dicho programa correctamente.

Contenido: Todos los tipos de información o datos que se divulguen a través de los diferentes servicios informáticos, entre los que se encuentran: textos, imágenes, video, diseños, software, animaciones, etc.

Contraseñas: Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.

Copia de respaldo o Backup: Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.

Correo electrónico institucional: Servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos, que se encuentra alojado en un hosting de propiedad de la Entidad.

Cuenta de acceso: Colección de información que permite a un usuario identificarse en un sistema informático o servicio, mediante un usuario y una contraseña, para que pueda obtener seguridad, acceso al sistema, administración de recursos, etc.

Disponibilidad: Se debe entender como la condición de acceso a la información y a los activos asociados cuando las personas, entes, procesos o aplicaciones lo requieren.

Dispositivos/Periféricos: Aparatos auxiliares e independientes conectados al computador o la red.

Dominio: Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red.

Espacio en disco duro: Capacidad de almacenamiento de datos en la unidad de disco duro.

Herramientas ofimáticas: Conjunto de aplicaciones informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionadas.

Información confidencial: Se trata de una propiedad de la información que pretende garantizar el acceso sólo a personas autorizadas.

Información/Documento electrónico: Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares. Se pueden clasificar por su forma y formato en documentos ofimáticos, cartográficos, correos electrónicos, imágenes, videos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, entre otros.

Información: La información es un activo que tiene valor, -que puede estar representada en forma impresa o escrita en papel, que puede estar almacenada física o electrónicamente, y que puede ser trasmitida por correo o medios electrónicos, por ende, requiere de una adecuada protección ante posibles vulnerabilidades que puedan afectar a la entidad de forma negativa.

Integridad Se debe entender como la propiedad que busca mantener y proteger la exactitud y estado completo de la información; y garantizar métodos de procesamiento libres de modificaciones no autorizadas.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Licencia de uso: Contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario (usuario consumidor/usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas, es decir, es un conjunto de permisos que un desarrollador le puede otorgar a un usuario en los que tiene la posibilidad de distribuir, usar y/o modificar el producto bajo una licencia determinada.

Mantenimiento físico preventivo: Actividad de limpieza de elementos como polvo, residuos de alimentos y otro tipo de partículas que debe realizarse sobre el equipo de cómputo, con el propósito de posibilitar que su correcto funcionamiento sea más prolongado en el tiempo.

Mantenimiento lógico preventivo: Es el trabajo realizado en el disco duro del equipo de cómputo, con la finalidad de mejorar el rendimiento general del sistema operativo.

Medios de almacenamiento extraíble: Son aquellos soportes de almacenamiento diseñados para ser extraídos del computador sin tener que apagarlo. Por ejemplo, memorias USB, discos duros externos, discos ópticos (CD, DVD), tarjetas de memoria (SD, Compact Flash, Memory Stick).

Plataforma web: Sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando a los usuarios la posibilidad de acceder a ellas a través de Internet.

Política: Compendio de directrices que representan una posición de las directivas, para áreas de control específicas que permiten establecer un canal de actuación en relación con los recursos y servicios de la entidad, normalmente soportadas por estándares, mejores prácticas, procedimientos y guías.

Propiedad intelectual: Se relaciona con las creaciones de la mente como invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. Es el conjunto de derechos que corresponden a los autores y a otros titulares.

Recurso informático: Todos aquellos componentes de Hardware y programas (Software) que son necesarios para el buen funcionamiento de un computador o un sistema de gestión de la información. Los recursos informáticos incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.

Red de datos: Es un conjunto de ordenadores que están conectados entre sí, y comparten recursos, información, y servicios.

Riesgo: El Riesgo se considera como todo tipo de vulnerabilidades, amenazas que pueden suceder.

Seguridad de la Información: La Seguridad de la Información tiene como finalidad la protección de la Confidencialidad, Integridad y Disponibilidad de la información, en cualquier presentación: electrónicos, impresos, audio, video u otras formas, ante accesos, usos, divulgación, interrupción o destrucción inadecuada y/o no autorizada de la información, las plataformas tecnológicas y los sistemas de información.

Seguridad Informática: La seguridad informática en el área de la informática, está concebida y enfocada a la protección de la información, los activos informáticos, la infraestructura tecnológica y los usuarios.

Seguridad: La Seguridad determina los riesgos y pretende mitigar los impactos mediante el establecimiento de programas en seguridad de la información y el uso efectivo de recursos; es un proceso continuo de mejora y debe garantizar que las políticas y controles establecidos para la protección de la información sean revisados y adecuados permanentemente ante los nuevos riesgos que se presenten.