Política de Seguridad de la Información Digital

SEGURIDAD DE LA INFORMACIÓN DIGITAL

GERENCIA DE SISTEMAS DE INFORMACIÓN

ALCALDÍA DISTRITAL DE BARRANQUILLA

NOVIEMBRE DE 2016

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL

Tabla de contenido

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL

1. INTRODUCCIÓN

La información es un activo que la Alcaldía Distrital de Barranquilla tiene el deber y la responsabilidad de proteger y salvaguardar de una manera segura, garantizando su disponibilidad, integridad y confidencialidad, la cual es esencial para proporcionar servicios eficientes a los ciudadanos.

La Alcaldía Distrital de Barranquilla tiene la responsabilidad de proteger la información y prevenir su mal uso tomando como marco de referencia lo establecido en las leyes 1273 de 2009, 1581 de 2012, 1712 de 2014, el Decreto 1377 de 2013 y la norma ISO 27001 para establecer políticas de seguridad que garanticen la confidencialidad de la información personal de los ciudadanos, empleados, directivos, proveedores y, en general, información relacionada con sus propias operaciones.

1.1 OBJETIVOS

- Establecer las directrices a seguir para el adecuado uso de los servicios y recursos de tecnología informática asignados a los usuarios de la ALCALDÍA DISTRITAL DE BARRANQUILLA, para el ejercicio y cumplimiento de sus funciones.
- Regular el uso de los servicios de correo y acceso a Intranet e Internet.
- Proteger la información de la Alcaldía de Barranquilla de todas las amenazas, ya sean internas o externas, deliberadas o accidentales.
- Permitir el intercambio de información segura.
- Promover que todo empleado, funcionario, contratista y demás personas que tengan relación con la alcaldía, tenga claro su rol en el uso y la protección de la información, con el fin de minimizar el riesgo de situaciones de responsabilidad legal ante un uso inadecuado de la información.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de los ciudadanos, proveedores y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Garantizar la continuidad operativa de la Entidad frente a incidentes.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL

1.2 ALCANCE

En esta Política de Seguridad de la Información se describe el marco de referencia para la gestión de Seguridad de la información digital de la Alcaldía de Barranquilla.

1.3 ÁMBITO DE APLICACIÓN

Esta Política de Seguridad de la Información digital, junto con sus normas, procesos y procedimientos se aplican a todos las personas, funcionarios, contratistas y demás agentes del estado que tienen acceso a los sistemas de información de la Alcaldía de Barranquilla. Estos lineamientos se extienden a los recursos tecnológicos (computadores y teléfonos, entre otros) que se conecten a la red de comunicaciones del Distrito de Barranquilla y cuyas actividades sean responsabilidad de funcionarios de la Alcaldía Distrital de Barranquilla.

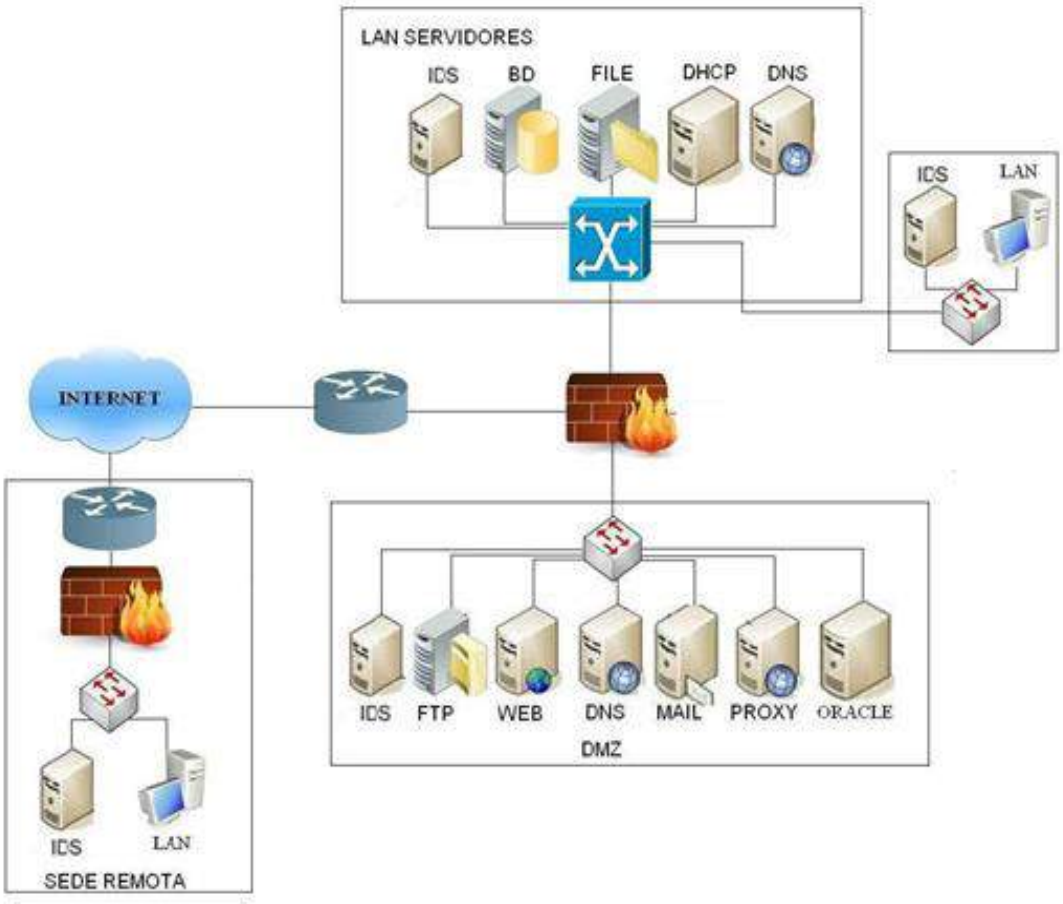
La política de seguridad de la información aplica a todas las formas de información, incluyendo:

- Comunicaciones enviadas por correo electrónico.
- La almacenada y procesada a través de servidores, computadores, portátiles, Tablet.
- La almacenada en cualquier tipo de medios extraíbles, CD, DVD, cinta, memoria USB, tarjetas de memoria, cámaras digitales.

1.4 ESQUEMA DE SEGURIDAD

Estas Políticas están enfocadas a salvaguardar y mantener disponible la información que maneja la entidad, garantizando la continuidad de su operación. Para lograr este fin se diseñó el siguiente esquema de seguridad que busca proteger la información, tanto de agentes externos como internos:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL



2. TÉRMINOS Y DEFINICIONES

Para los fines de este documento, los términos y definiciones empleados son los siguientes:

Sistema de Gestión de la Seguridad de la Información (SGSI): corresponde al diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Usuarios: el usuario es aquella persona que usa una cosa o servicio habitualmente. En sentido general, un usuario es un conjunto de permisos y de recursos a los cuales se tiene acceso.

Confidencialidad: es la cualidad de la información por medio de la cual se garantiza que está disponible únicamente al personal autorizado para acceder a dicha información.

Seguridad informática o **de tecnologías de la información:** es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta; especialmente la información contenida o circulante. Para ello existe una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo en el supuesto de que esta información confidencial llegue a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

Hardware: conjunto de los componentes que integran la parte material de una computadora

Software: son los programas informáticos que hacen posible la realización de tareas específicas dentro de un computador

Base de Datos: se puede definir como un conjunto de información relacionada que se encuentra agrupada o estructurada.

Metadatos: Los metadatos son datos altamente estructurados que describen información, el contenido, la calidad, la condición y otras características de los datos. Es "Información sobre información" o "datos sobre los datos". El término metadatos describe varios atributos de los objetos de información y les otorga significado, contexto y organización.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL

Archivo o **fichero informático:** es un conjunto de bits que son almacenados en un dispositivo. Un archivo es identificado por un nombre y la descripción de la carpeta o directorio que lo contiene. A los archivos informáticos se les llama así porque son los equivalentes digitales de los archivos escritos en expedientes, tarjetas, libretas, papel o microfichas del entorno de oficina tradicional.

Integridad: es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Es la acción de mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

Disponibilidad: es la propiedad de estar accesible y utilizable al ser solicitado por una entidad autorizada.

Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Activos: cualquier cosa que tenga valor para la organización es considerada un activo en este caso la información es un activo.

Control: los medios de gestión de riesgos, incluidas las políticas, procedimientos, directrices y prácticas.

Política: su objetivo es establecer, a partir de la observación de hechos de la realidad política, principios generales acerca de su funcionamiento.

Riesgo: riesgo es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

Terceros: persona o entidad que se reconoce como independiente.

Amenaza: causa potencial de un incidente no deseado, que puede producir un daño a un sistema.

Vulnerabilidad: debilidad de un sistema que puede ser explotada por una o más amenazas.

Malware: código maligno, software malicioso, software dañino o software malintencionado. Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario

3. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La alcaldía Distrital de Barranquilla garantiza la seguridad de la información fundamentada en la correcta gestión de los activos de información identificando su ciclo de vida asegurando lo siguiente:

- **Confidencialidad**: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados; se encuentra resguardada o salvaguardada en nuestros centros de datos con control de acceso a los usuarios a cada información.

- **Integridad**: se realiza el mantenimiento de la exactitud y completitud de la información y sus métodos de procesamiento para la actualización y revisión, así como los responsables del mismo en cada uno de los procesos que maneja la entidad.

- **Disponibilidad**: el acceso y utilización de la información y los sistemas por parte de los individuos, entidades o procesos autorizados permanentemente o según lo requieran.

4. RIESGOS Y CONTROLES DE SEGURIDAD

La información puede estar en peligro por el uso indebido y la vulnerabilidad de los controles de seguridad, igualmente los incidentes de seguridad de la información pueden originar pérdida de prestigio y desconfianza, pérdida financiera, no cumplimiento de las normas y la legislación, así como posibles demandas judiciales en contra de la Alcaldía.

Teniendo en cuenta los riesgos a los que está expuesta la Alcaldía Distrital de Barranquilla, permanentemente se realiza un análisis sobre la posibilidad de ocurrencia de estos, se implementan y ajustan los controles que buscan reducir la ocurrencia de los mismos; los cuales generarían un impacto sobre los objetivos institucionales.

4.1 GESTIÓN DE RIESGOS

Se tienen identificados dos tipos de riesgo que se pueden presentar en la entidad, tales como riesgo externo y riesgo interno.

- Los riesgos externos son todos aquellos eventos de intento de acceso a la información sin la respectiva credencial o permiso a usuarios externos a la red local y WAN de la Alcaldía Distrital de Barranquilla. Para esto se cuenta con un equipo de seguridad perimetral que protege los servicios publicados tales como la página web, aplicaciones web y otros productos abiertos a la ciudadanía.

- Los riesgos internos son todos aquellos eventos de intento de acceso a la información sin la respectiva credencial o permiso desde el interior de la red local y WAN de la Alcaldía Distrital de Barranquilla. Para esto se cuenta con un controlador de dominio que permite implementar políticas de permisos y restricciones de acceso a los usuarios.

4.2 ACCIONES PARA CONTROLAR EL RIESGO

Garantizar un nivel de protección total de la información es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de nuestro sistema de gestión de la seguridad de la información es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la Entidad de una forma documentada, estructurada, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Teniendo en cuenta lo anterior, la Alcaldía Distrital de Barranquilla lleva a cabo las evaluaciones y verificaciones para identificar, cuantificar, priorizar y controlar los riesgos.

Los controles implementados son seleccionados estratégicamente para mitigar los riesgos identificados**.**

4.3 PROTOCOLOS DE SEGURIDAD DE LA INFORMACIÓN

Los protocolos de seguridad son un conjunto de reglas que se administran dentro de la transmisión de datos entre la comunicación de dispositivos, con el propósito de ejercer la confidencialidad, integridad y autenticación de la información.

La red telemática y la información que maneja el Distrito de Barranquilla se encuentra protegida por herramientas que procuran su confidencialidad e integridad.

4.3.1 Equipo de Seguridad Perimetral

El Distrito de Barranquilla cuenta con una herramienta de seguridad perimetral que establece un radio o zona de seguridad en los accesos a la red interna e internet; esta herramienta se encuentra alojada en el centro de cómputo con los demás equipos de comunicaciones.

El equipo de seguridad que forma parte de la red es un Firewall de última tecnología, que se encarga entre otras funciones de:

- Impedir la entrada de ataques o accesos de intrusos desde el exterior mediante filtrado de contenido, filtrado de URL, modelo de políticas unificadas, análisis basados en firmas, lista de exclusiones de IPS's, algoritmos para expresiones regulares, puerta de enlace con funcionalidad antipsyware mediante el protocolo H.323 y manejo de protocolos comunes, tales como HTTP / S, FTP, SMTP, SMBv1 / v2 y otros, que no envían los datos en TCP simple, y decodifica las cargas útiles para la inspección de malware.
- El firewall utiliza para su función de enrutamiento trayectos estáticos, tabla de políticas y protocolos BGP, OSPF, RIPv1/v2.
- Los accesos VPN para trabajo remoto están basados en comunicación encriptada mediante los protocolos SHA-1, DES, 3DES, AES (128, 192, 256-bit)/MD5, con intercambio de llaves empleando el protocolo criptográfico Diffie Hellman Groups 1, 2, 5, 14.

4.3.2 Gestión de Seguridad de la Red LAN

Existe una política de acceso por MAC registrada, lo cual no permite conectar equipos tales como switch, routers, access point, portátiles, tablets, celulares o cualquier otro

dispositivo a la red de la Alcaldía Distrital de Barranquilla sin previa autorización de la Gerencia de Sistemas de Información.

El equipo que requiera estar conectado a la red de datos del Distrito debe ser registrado con anterioridad para que pueda ser conectado.

4.3.3 Protección Contra Software Malicioso

Para la protección interna de la información se cuenta con un Antivirus administrado desde una consola central que permite la restricción de accesos a sitios Web no autorizados y mantiene actualizada diariamente la base de datos para detección inmediata de código malicioso que intenta ingresar a nuestros equipos y servidores.

La herramienta de seguridad perimetral cuenta adicionalmente con un motor anti malware que permite controlar los ataques internos y externos

4.3.4 Incidentes de seguridad

Evaluar el tipo de vulnerabilidad detectado e identificar el tipo de incidente, sobre los siguientes tipos de ataques posibles:

- Spoofing: este tipo ataque consiste en suplantar o falsificar un portal. Para esto es necesario monitorear los servidores de gestor de contenidos (ej: joomla, wordpress, etc). Una vez se identifique si hubo una vulnerabilidad se eliminan los archivos que crean el spoofing y se restringen los permisos en la carpeta donde se ubicaron dichos archivos.

- DoS : Este ataque se define como Denial of Service y consiste en saturar los procesos de un portal y/o servidor mediante peticiones, las cuales provocan que se incrementen el consumo de recursos de los servidores causando así que se saturen y evitando la caída de mismo. Esto se detecta mediante el monitoreo de los recursos del servidor. Si se observa un consumo de recursos pico, se identifica de donde provienen las peticiones. Una vez identificado su origen, se bloquea dicho origen a través del firewall mediante bloqueo de IP. Adicional a esto se implementa una herramienta que detecta bajo un parámetro establecido, cuántas peticiones debe recibir un servidor de forma regular. En caso de que este parámetro o umbral se supere, la herramienta rechaza todas las peticiones de la IP origen, como medida de seguridad.

Una vez evaluado el ataque e implementada una solución, se procede a efectuar procedimientos de mayor envergadura para que no se repitan dichos ataques.

Como medidas preventivas, en el firewall se implementan políticas de seguridad más agresivas. Se realiza restricción de puerto en general dejando como excepción los puertos por el cual los servicios están publicados. Se eliminan o se restringen accesos a los servidores mediante cambio de contraseñas de manera más frecuente y se eliminan permisos de escritura sobre determinadas carpetas del servidor.

4.3.5 Gestión de acceso de los usuarios

Los usuarios que utilizan aplicaciones u otro tipo de información sensible se les hacen entrega de credenciales para el acceso a estas. Las claves de acceso deben contener las siguientes características que permitan ser más seguras:

- Crea contraseñas que tengan al menos 8 caracteres o más.
- Nunca utilizar solo números.
- Optar siempre por combinaciones alfanuméricas, letras mayúsculas y minúsculas, números e intercalar con caracteres especiales o símbolos del teclado.
- No usar la misma contraseña para sitios web distintos.
- Crea contraseñas que sean fáciles de recordar pero difíciles de adivinar para los demás.
- No mantener una misma contraseña indefinidamente.
- Cambiarla regularmente.

La clave es individual, personal, secreta e intransferible. Al momento de efectuar las transacciones, esta permite registrar a los responsables de cualquier cambio. A continuación se describen las recomendaciones generales sobre el uso de las claves:

- Tener cuidado al momento de digitar la clave, asegurándose de que no lo observen así como usted no debe observar a otros mientras lo hacen.
- No compartir ni pedir la clave a nadie.
- No escribir la clave en papel ni guardarla en un archivo sin cifrar. En caso de hacerlo, no dejarla al alcance de terceros (debajo del teclado, en un cajón del escritorio, etc.) y NUNCA pegada al monitor.
- No habilitar la opción de “recordar claves” en los programas utilizados.
- No enviar la clave por correo electrónico o chat, no mencionarla en conversaciones presenciales o telefónicas, ni entregarla a nadie, aunque sea o diga ser el administrador del sistema.
- Cambiar la Clave si existe alguna sospecha de que alguien puede conocerla. Poner en conocimiento al administrador de la red o aplicativo de cualquier incidente que ocurra con la cuenta.
- En caso de olvidar la clave debe contactar al administrador del sistema.

- En caso de acceder a algún servicio o correo electrónico en un lugar público, tenga en cuenta la posibilidad de que la clave haya podido ser espiada o comprometida, por lo que se recomienda cambiarla.
- Cerrar las sesiones abiertas cuando no se estén utilizando.

Es responsabilidad de los usuarios salvaguardar sus credenciales de acceso a sistemas operativos, aplicaciones, bases de datos y correo. Los usuarios no deben compartir estas credenciales.

4.3.6 Requerimientos y servicios de los usuarios

Los usuarios cuentan con una herramienta para realizar las solicitudes sobre sus necesidades de sistemas a través de una herramienta de gestión de activos y fallos (GLPI) para administrar, atender y gestionar los requerimientos y servicios.

5. POLÍTICA DE SEGURIDAD

La Política de Seguridad de la Información hace referencia a los lineamientos establecidos por la ADMINISTRACIÓN DISTRITAL DE BARRANQUILLA con respecto a la protección de los activos de información. La ALCALDÍA DISTRITAL DE BARRANQUILLA ha decidido definir e implementa
r unas Políticas de Seguridad de la Información, soportados en lineamientos claros según las necesidades de la Entidad y los requerimientos legales vigentes.

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores y terceros.

5.1 USO DE LA TECNOLOGÍA Y PROPIEDAD DE LA INFORMACIÓN

Los usuarios deben tener claridad acerca de que la información que tienen a su cargo y manejan a través de un sistema informático dentro del ejercicio de sus funciones, es propiedad de ALCALDÍA DE BARRANQUILLA.

a) Todos los usuarios son responsables del uso adecuado de la información que manejan y tienen el criterio suficiente para asumir las consecuencias de darle una destinación personal o en contra de lo ajustado a la Ley. De igual forma, los recursos tecnológicos asignados como el acceso a Internet y el correo electrónico son exclusivos para ejercer funciones de trabajo. Si un usuario tiene dudas sobre el uso de un recurso o información de ALCALDÍA DE BARRANQUILLA, se sugiere consultar al departamento de Sistemas antes de proceder con la acción a ejecutar.

b) Es responsabilidad de los usuarios que manejan información confidencial y sensible de la ALCALDÍA DE BARRANQUILLA, dar el tratamiento que propenda por su protección, y hacer uso de herramientas criptográficas y certificados electrónicos en transacciones vía WEB o correos electrónicos previamente proporcionados por la entidad.

c) Para propósitos de mantenimiento de la red y de seguridad, las personas autorizadas dentro de la Alcaldía podrán monitorear equipos, sistemas y tráfico de red en cualquier momento, y tienen el compromiso de informar todo incumplimiento de las normas de buen uso de los recursos si detectasen anomalías que pongan en riesgo la información de la entidad o atenten contra la continuidad de su operación normal.

d) Dado que los computadores asignados a los usuarios son administrados por LA ALCALDÍA DE BARRANQUILLA o sus ENTIDADES ADSCRITAS, la Alcaldía se

reserva el derecho de revisarlos o auditarlos periódicamente, así como las redes y los sistemas, sin previo aviso y sin necesidad de autorización por parte de la comunidad de usuarios para garantizar el cumplimiento de esta política. En cualquier caso la persona encargada de la revisión o auditoría del computador será designada por el Gerente de Sistemas de Información en conjunto con el Jefe del área auditada.

e) Solo tendrán acceso a los sistemas de Información aquellos usuarios que por sus funciones así lo requieran, con el visto bueno de su jefe inmediato, del usuario líder responsable del sistema de información correspondiente y del Jefe de la Gerencia de Sistemas.

5.2 SEGURIDAD DE LA INFORMACIÓN

La información que manejan los usuarios y que es crítica para la ALCALDÍA DE BARRANQUILLA, debe ser protegida y respaldada por procedimientos que son responsabilidad de los usuarios. El departamento de Sistemas velará por la información que se encuentra en los servidores ubicados en el Centro de Cómputo y el usuario por su parte, custodiará la información almacenada en su computador.

Para cumplir con esta premisa, es importante tener en cuenta lo siguiente:

a) La interfaz de usuario para acceder a la información disponible en los sistemas debe tener restricciones de acceso y es responsabilidad de cada usuario prevenir el ingreso de personal no autorizado a los sistemas desde los recursos que le son asignados por la ALCALDÍA DE BARRANQUILLA.

b) El usuario es responsable de la seguridad de las cuentas que le son asignadas y la confidencialidad de claves asociadas, así como de cumplir con las condiciones de cambio y conformación que imponga cada aplicativo. Todas las actividades que se realicen con una identificación son responsabilidad del funcionario al que le fue asignada. Por ello, está totalmente prohibido ceder y dar a conocer las claves a un tercero.

c) Es obligación de los Jefes de área, verificar permanentemente el nivel de acceso de sus funcionarios a la información de la entidad manejada a través de Sistemas de información. Cualquier cambio en los niveles de acceso existentes debe solicitarse a la Gerencia de Sistemas de Información.

d) Todos los computadores portátiles y estaciones de trabajo deben tener configurados un protector de pantalla con clave y con un tiempo de espera máximo de 5 minutos

para bloquear el acceso cuando el equipo esté desatendido. Es responsabilidad de cada usuario bloquear el equipo sin esperar la activación del protector de pantalla, si sabe que se ausentará de su puesto de trabajo.

e) Debido a que la información contenida en computadores portátiles presenta un alto riesgo de vulnerabilidad, los usuarios se comprometen a tener especial cuidado tanto con el equipo, como con la información contenida en el mismo. En caso de que LA ALCALDÍA DE BARRANQUILLA le proporcione al usuario una aplicación de criptografía para impedir el acceso sin restricciones a la información, el usuario está en la obligación de emplearla para proteger la confidencialidad e integridad de la información.

g) Todos los equipos conectados a la red de comunicaciones de la ALCALDÍA DE BARRANQUILLA, aunque sea propiedad de la persona que lo utiliza, deben ejecutar regularmente el software de antivirus aprobado por la entidad con la base de datos de virus actualizada a la fecha, así como tener legalizado el licenciamiento del sistema operativo y todas las aplicaciones contenidas en el equipo. Se sugiere a todos los usuarios revisar la fecha de la base de datos del software de antivirus y reportar a la Gerencia de Sistemas si encuentra una diferencia mayor a una semana con respecto a la fecha actual. Si el computador no tiene instalado el antivirus permitido por la ALCALDÍA DE BARRANQUILLA, debe solicitar la instalación al personal del Departamento de Sistemas antes de ser conectado a la red de datos.

i) La digitación de la clave, ya sea en el ingreso a un sistema o por cambio de la misma, debe realizarse de tal forma que no sea conocida por un tercero.

j) Evite el uso de claves fáciles de deducir en todas las plataformas a las que acceda (ejemplo: nombre de un hijo, equipo de fútbol, etc.). Así mismo evite utilizar patrones cuando cambia su clave (ejemplo: clave1; clave2; clave3; 12345; etc.). Utilice claves que sean fáciles de recordar para usted, pero difícil de descifrar para otros, por ejemplo, claves de 6 caracteres o más; es recomendable combinar letras (mayúsculas y minúsculas) y números

5.3 ACCESO A CENTRO DE DATOS Y SERVIDORES

El acceso a los servidores para su administración está a cargo del personal de la Gerencia de Sistemas de Información asignados a la seguridad del Centro de Datos. Estos no deben compartir las contraseñas de acceso, las cuales deben ser cambiadas al menos tres (3) veces al año.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL

El acceso al centro de datos es restrictivo, ya que solo es posible bajo autorización de la Gerencia de Sistemas de Información. Cuando se realice este acceso por parte de un personal externo al área por motivos de revisión, mantenimiento de los servidores o plantas debe hacerse bajo la supervisión de uno de los funcionarios encargados de la seguridad del Centro de datos adscrito a la Gerencia de Sistemas de Información.

5.4 COPIAS DE SEGURIDAD (BACKUP)

Esta política define la estrategia de copia de Seguridad de Información y de las aplicaciones de la Alcaldía de Barranquilla. El objetivo de la política es asegurarse de obtener un respaldo de la información contenida en los servidores a fin de que, en caso de una eventualidad, se pueda continuar con la operación de la entidad.

a) La información de los servidores y demás sistemas serán respaldados mediante un método de copia de seguridad adecuado, igualmente, se debe utilizar un medio de almacenamiento apropiado, puede ser cinta o cualquier otro medio reconocido.

b) El estado de las copias de seguridad que se realizan a diario son auditadas para identificar y corregir los defectos y/o inconsistencias encontradas.

c) Para las copias de seguridad se utiliza el método de rotación Abuelo-Padre-Hijo (GFS - Grandfather, Father, Son) realizadas diaria, semanal y mensualmente, o un método simple de rotación diaria. Cuando un método simple de rotación diaria se utiliza, se mantiene un mínimo de 7 copias de seguridad hasta cumplir tres meses, cuando se reinicia la rotación.

d) Las unidades grabadoras utilizadas para realizar las copias de seguridad se deben limpiar con regularidad.

e) Para el almacenamiento de las copias de seguridad se deben tener en cuenta los siguientes criterios:
   - Los medios de copia de seguridad se almacenan de forma segura cuando no estén en uso.
   - Los medios extraíbles se almacenan de forma segura en una caja de seguridad contra incendios, cuando no están en uso.

f) Las copias de seguridad de servidores y aplicaciones, como mínimo, deben cumplir con las siguientes pautas:

Servidor / Aplicación	**Ciclo de copia de seguridad**	**Medios**
Servidor de Aplicaciones	Mensual	Cinta / Disco externo
Servidor de Mensajería	Diaria	Cinta / Disco externo
Servidores de Bases de Datos	Diaria	Cinta / Disco externo

Firewall	Semanal	Disco externo
Network Switches	Anual	Disco externo
Planta Telefónica	Mensual	Disco externo
Base de Datos GLPI	Semanal	Disco Externo

5.5 SEGURIDAD DE LA PLANTA TELEFÓNICA

El sistema de telecomunicaciones de la alcaldía está conformado por una planta telefónica PANASONIC KXTDE600 con un módulo de expansión KXTDE620, lo cual nos permite tener capacidad para 200 extensiones telefónicas.

Este sistema es administrado por la Gerencia de Sistemas desde donde se realiza la administración del equipo, dentro de las tareas de administración de la planta se encuentran la asignación, traslados, configuración de privilegios de todas las extensiones. El backup del sistema se realiza con una periodicidad mensual.

5.6 SEGURIDAD DE LA ESTACIÓN DE TRABAJO

La ALCALDÍA DE BARRANQUILLA asigna Estaciones de trabajo (computadores, impresoras y cualquier otro dispositivo electrónico) a los funcionarios que lo requieren para que ejecuten labores propias del cargo. El usuario debe cuidar estos activos que tiene bajo su responsabilidad y utilizarlos exclusivamente para labores relacionadas con su trabajo, no debe usarlo para otros fines.

5.6.1 Protección contra la intemperie

Los usuarios velarán para que los computadores de escritorio y portátiles; así como los que tenga a su disposición estén protegidos contra la intemperie, en especial aquellos que se encuentren ubicados en sitios expuestos a polvo y humedad o que por razones de brigadas o actividades propias de cada dependencia, tengan que trasladarse a sitios distintos a donde fueron instalados para su habitual funcionamiento.

5.6.2 Corriente Regulada

En los puestos de trabajo donde exista un circuito eléctrico regulado, los usuarios de equipos electrónicos de cómputo tales como computadores de escritorio, portátiles y equipos de telecomunicaciones (Access Point, Switches) serán responsables por la adecuada conexión de sus equipos a tomas eléctricas reguladas, las cuales se identifican con el color naranja. No debe conectarse ningún otro dispositivo, tales como impresoras, radios, cargadores de celulares, fotocopiadoras, televisores, abanicos, etc., porque podrían

causar sobrecarga en los circuitos y potencialmente producir daño físico de los computadores.

5.6.3 Mantenimiento preventivo y toma de inventarios

Todos los usuarios deben facilitar el acceso a sus equipos, cuando el departamento de Sistemas programe mantenimiento preventivo o revisión de información para inventarios.

5.7 UTILIZACIÓN DEL CORREO ELECTRÓNICO, ACCESO A INTERNET E INTRANET

Esta política pretende garantizar el uso efectivo del tiempo laboral, evitando el uso inapropiado del correo electrónico, internet e intranet.

El correo electrónico es proporcionado al personal con el objetivo de ayudarle a llevar a cabo sus funciones de manera eficiente y eficaz, permitiendo la comunicación con los demás miembros del personal, otras empresas y entidades asociadas. El acceso a Internet en la Alcaldía de Barranquilla está controlado por las políticas internas de la seguridad de la información.

Los servicios de correo electrónico, internet e intranet de la Alcaldía de Barranquilla son para uso laboral; no debe ser utilizado para temas personales.

5.7.1 Uso del correo electrónico

a) Cuando se utilizan los medios electrónicos de la Alcaldía de Barranquilla para el acceso al correo electrónico, debe cumplirse con las siguientes pautas:
   - Consultar su correo electrónico diariamente.
   - Incluir una línea de asunto significativo en su mensaje.
   - Comprobar la línea de dirección antes de enviar un mensaje y verificar que lo envíe a la persona adecuada.
   - Respetar las protecciones legales a los datos y software proporcionados por derechos de autor y licencias.

b) La herramienta de correo electrónico utiliza un filtro corporativo para evitar que se reciba contenido malicioso.

c) Todos los mensajes de correo electrónico emitidos por usuarios de ALCALDÍA DE BARRANQUILLA o sus entidades adscritas que sean dirigidos a direcciones de correo externas, que contengan información confidencial, deben incluir una nota (Disclaimer) como la que se muestra a continuación:

La información contenida en este mensaje es confidencial y tiene como único destinatario la persona a quien está dirigida.
La Alcaldía de Barranquilla ha implementado un sistema para el control de virus, sin embargo, no asume ninguna responsabilidad por virus que pueda llevar este mensaje o sus anexos.

d) Los usuarios de la red de ALCALDÍA DE BARRANQUILLA deben abstenerse de abrir archivos adjuntos de correo electrónico, recibidos de remitentes desconocidos o sospechosos ya que pueden contener virus

e) Todos los correos electrónicos entrante y saliente son analizados por el antivirus (antimalware), para identificar mensajes maliciosos y su utilización.

f) El uso de herramientas de mensajería instantánea diferente a la autorizada, está prohibido desde los computadores y redes de la Alcaldía. Así mismo están prohibidos la transferencia de datos y el registro de los mensajes, por este tipo de herramientas.

g) Constituye un delito suplantar personas a través de correo electrónico y enviar mensajes en nombre de terceros.

h) La suscripción a listas de correo electrónico y redes sociales para fines personales no está permitida. Así mismo la entrega de listas cuentas de correo instituciones a terceros para fines comerciales.

i) Debido a que el correo electrónico es una herramienta institucional, la información enviada debe mantener este carácter, por lo tanto los mensajes de índole personal y que no guarden relación con el ejercicio de las funciones asignadas no deben generarse a través de esta plataforma.

5.7.2 Acceso a Intranet e Internet

a) El uso personal y razonable de Internet está permitido en su tiempo libre; pero, sujeto a las condiciones establecidas en las políticas de seguridad de la Alcaldía de Barranquilla.

b) Cuando se utilizan las instalaciones de la Alcaldía de Barranquilla para acceso a Internet debe cumplir con las siguientes pautas:
   - Hacer respetar la protección legal a los datos y el software proporcionado por derechos de autor y protección de datos.
   - Informar a la Gerencia de Sistemas inmediatamente observe cualquier acontecimiento inusual.

- No está permitido el acceso de contenido para adulto (pornografía y juegos)

c) Un filtro corporativo de Internet se utiliza para prevenir tipos específicos de sitios web que se accede. Si un usuario necesita acceder a un sitio web que está bloqueado o restringido, el jefe inmediato debe solicitar por los canales de comunicación establecidos, la respectiva autorización a la Gerencia de Sistemas.

d) El historial de acceso a Internet es monitoreado, permitiendo identificar los sitios visitados por los usuarios, lo cual puede ser utilizado durante investigaciones cuando se sospeche el uso indebido del recurso.

e) Los usuarios no están autorizados para descargar programas o software (incluyendo protectores de pantalla y fondos de escritorio) de la Internet. Si se requieren programas disponibles en Internet para realizar funciones propias de la Alcaldía, es necesario ponerse en contacto con la Gerencia de Sistemas que hará las gestiones necesarias para adquirir y disponer la instalación de los mismos.

f) La intranet es una herramienta de comunicación interna utilizada para brindar información sobre las actividades, documentación institucional y trámites exclusivos de los funcionarios de la Alcaldía de Barranquilla. Se recomienda consultar diariamente la información publicada para mantenerse informado, dar un uso adecuado a los trámites ofrecidos desde la intranet y utilizar la documentación institucional publicada para los fines pertinentes

5.8 USOS INADECUADOS DE LAS HERRAMIENTAS TECNOLÓGICAS (PROHIBICIONES)

Bajo ninguna circunstancia se justifica el uso de los recursos informáticos en la ejecución de actividades prohibidas por las normas de la entidad, jurídicas, nacionales o internacionales, incluyendo todas aquellas que protegen los derechos de autor.

Para mayor claridad sobre las actividades consideradas de uso inadecuado, se clasifican en el siguiente aparte alguna de ellas.

5.8.1 Usos Inadecuados en los Sistemas y de la Red

a) Violaciones de los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual. Entre otras actividades se incluye la distribución o instalación de software sin la licencia de uso adquirida por ALCALDÍA DE BARRANQUILLA o sin la debida autorización de la Gerencia de Sistemas de la entidad.

b) Emplear los computadores asignados para el ejercicio de sus funciones para almacenar material ofensivo contra la moral, la dignidad y el bienestar de terceros, como pornografía, injuria o cualquier información de amenazas.

c) Copia no autorizada de material protegido por derechos de autor que incluye, digitalización y distribución de imágenes o fotografías de cualquier origen (revistas, libros, páginas web, etcétera), digitalización y distribución de música, audio o video, distribución e instalación de software ilegales.

d) Exportar o copiar software elaborado o adquirido por la ALCALDÍA DE BARRANQUILLA, información técnica o relevante de la operativa diaria, sin previa autorización escrita de un superior o área responsable.

e) Instalación de software malicioso en los equipos de la red o en los servidores, así como software y tecnologías para criptografía en contra de leyes de controles.

f) Revelar la clave de su cuenta de acceso de las aplicaciones a otras personas (correo electrónico, aplicaciones internas, etc.) o permitir su uso a terceros para actividades ajenas a la misión de la ALCALDÍA DE BARRANQUILLA a menos que exista explícitamente una autorización para ello, la cual debe formalizarse por escrito. (La prohibición no debe contemplar excepciones, aunque estas se den con la autorización de los jefes)

g) Desarrollar aplicaciones con fines personales o comerciales utilizando la infraestructura tecnológica de la ALCALDÍA DE BARRANQUILLA.

h) Utilizar la infraestructura de tecnología de información de la ALCALDÍA DE BARRANQUILLA para conseguir o transmitir material con ánimo de lucro.

i) Se prohíbe el uso del sistema de comunicaciones de la ALCALDÍA DE BARRANQUILLA con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil hacia personas naturales o jurídicas, dentro o fuera del territorio nacional.

j) Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios tecnológicos propios de la ALCALDÍA DE BARRANQUILLA o entidades adscritas.

k) Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios. Entre las acciones que contravienen la seguridad de la red se encuentran, aunque no están limitadas a estas, acceder a

datos cuyo destinatario no es usted, ingresar a una cuenta de un servidor o de una aplicación para la cual no está autorizado.

l) Está prohibido explícitamente el monitoreo de puertos o análisis de tráfico de red con el propósito de evaluar vulnerabilidades de seguridad. Las personas responsables de la seguridad informática pueden realizar estas actividades cuando se efectúen en coordinación con el personal responsable de los servidores, los servicios, las aplicaciones y de la red.

m) Intentar burlar los mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor, o cuenta de usuario.

n) Realizar cualquier acción cuya intención sea la de interferir, interrumpir o lesionar la continuidad de un servicio, la imagen de la ALCALDÍA DE BARRANQUILLA o infringir alguna norma o restricción estipulada en esta política.

o) Proporcionar a terceros información sobre aplicativos, configuraciones, y datos de manejo exclusivo de la ALCALDÍA DE BARRANQUILLA, sin la debida autorización.

p) Manejar negocios personales haciendo uso de los recursos de la Entidad.

5.8.2 Uso inadecuado del correo electrónico y sistemas de comunicación

a) Está prohibido:

- Enviar correos electrónicos cuyo contenido sea inapropiado, tales como mensajes que incluyan material comercial y/o publicitario no solicitado, sin importar el idioma, la periodicidad o tamaño del mensaje.
- Retransmitir cadenas electrónicas sin propósito laboral.
- Proporcionar la dirección de correo en las subscripciones a páginas Web de entretenimiento o de interés personal. Para este efecto se deben utilizar las cuentas de correo personales.
- Usar el correo de la entidad para enviar material pornográfico, o con cualquier contenido que viole derechos de autor o derechos humanos.
- Expresar puntos de vista que puedan ser considerados como difamatorios o injuriosos.

b) Se debe ser selectivo en cuanto a la información que se envía a través del correo, el envío de fotos, videos, archivos de sonido e imágenes, ya que estos archivos ocupan mucho espacio y congestionan tanto la red interna como el canal de Internet. Se deben utilizar herramientas de compresión de archivos cuando se requiera intercambiar archivos muy grandes como presentaciones, gráficos, tablas, etc. Si el

receptor es interno, el usuario debe utilizar las carpetas compartidas para estos efectos.

c) El envío de correos con información no relevante a múltiples receptores ya que estos ocupan mucho espacio y/o congestionan los recursos internos de manera innecesaria.

e) Imprimir mensajes de correo electrónico a menos que sea absolutamente necesario.

5.8.3 Uso inadecuado de internet

a) El ingreso a sitios reconocidos y de inapropiada reputación, el acceso a sitios con contenidos no apropiados tales como juegos, apuestas, pornografía, etc., son inaceptables, más aún, acceder, ver, bajar o reenviar material obsceno, amenazador, acosador explícito, chistes o comentarios degradantes es un uso no apropiado del equipo suministrado por la ALCADÍA DE BARRANQUILLA.

b) Utilizar la red de la Alcaldía de Barranquilla para conectar cualquier dispositivo, sin previa autorización.

c) Utilizar el acceso a Internet para publicar material difamatorio o injurioso.

5.8.4 Excepciones

Algunos miembros de ALCALDÍA DE BARRANQUILLA pueden estar exentos de seguir algunas de las restricciones enumeradas en los ítems anteriores debido a las responsabilidades de su cargo o a eventos no programados. Estas excepciones deben ser solicitadas a la Gerencia de Sistemas de Información con previa aprobación del Jefe de la Dependencia y no exoneran el cumplimiento de las leyes nacionales o internacionales vigentes.

5.9 ADQUISICIÓN, DESARROLLO, MANTENIMIENTO Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

El software que se adquiera y/o desarrolle debe cumplir con parámetros previos antes de su entrega, como son la necesidad de hardware que soporte y/o licencias en caso de ser necesarias. Una vez se haga entrega oficial, se asigna a un funcionario para su respectivo soporte.

6. MONITOREO

Se realiza una revisión periódica de todos los elementos como son los equipos de red, servidores y firewall para verificar su funcionamiento, en caso de detectar una falla o anomalía se toman los correctivos del caso. Estos eventos son recopilados en una bitácora para llevar un registro de las incidencias.

7. ROLES Y RESPONSABILIDADES

Todos los usuarios están sujetos a las políticas adoptadas para ello y a una actuación con altos principios morales y éticos al utilizar los recursos de la Alcaldía Distrital de Barranquilla.

Es responsabilidad de la Gerencia de Sistemas la difusión de esta política, así como la vigilancia y control en el uso de los recursos de redes e información contenidas en las Bases de Datos que administra y es deber de todos sus integrantes reportar cualquier infracción de la misma, sin importar de quien provenga.

Así mismo es deber de todos los funcionarios de la ALCALDÍA DE BARRANQUILLA y entidades adscritas el cumplimiento de esta política.

8. OTRAS CONDUCTAS RELACIONADAS CON SISTEMAS DE INFORMACIÓN QUE TAMBIÉN DAN LUGAR A INVESTIGACIONES DISCIPLINARIAS

El uso inadecuado de los equipos de cómputo de la Alcaldía Distrital de Barranquilla que están bajo la responsabilidad de cada servidor público o contratista en el ejercicio del cargo, podrá generar la apertura de un proceso disciplinario al amparo de la ley 734 de 2002, sin perjuicio de la responsabilidad penal que puedan acarrear dichas conductas.

9. REVISIÓN

La revisión de la presente política estará a cargo del Gerente de Sistemas de Información de la Alcaldía Distrital de Barranquilla y esta será revisada cuando se considere necesario; sin embargo, el periodo no debe ser superior a un año.

10. VALIDEZ DE LA POLÍTICA

La presente política es aplicable a partir de su aprobación.

11. REFERENCIAS

- https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba
- https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n
- https://www.ecured.cu/Usuario_(Inform%C3%A1tica)
- https://es.wikipedia.org/wiki/Confidencialidad
- https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
- https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n
- https://es.wikipedia.org/wiki/Hardware
- https://www.gcfaprendelibre.org/tecnologia/curso/informatica_basica/empezando_a_usar_un_computador/2.do
- http://www.maestrosdelweb.com/que-son-las-bases-de-datos/
- http://www.unal.edu.co/siamac/sig/metadatos1.html
- https://es.wikipedia.org/wiki/Archivo_(inform%C3%A1tica)

- http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf
- http://www.iso27000.es/sgsi.html
- https://es.wikipedia.org/wiki/Malware

12. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Fecha	**Versión**	**Descripción del Cambio**
10/11/2016	1.0	Se establece una nueva versión de la Política de Seguridad de la Información.