CONTRALORIA DISTRITAL DE BUENAVENTURA

POLÍTICAS DE SEGURIDAD INFORMÁTICA DE LA CONTRALORÍA DE BUENAVENTURA

JOSE ALFRFEDO LOBATO M

CONTRALOR DISTRITAL

Elaboro

WILLIAM TENORIO ANGULO

Profesional Universitario- Sistemas

TABLA DE CONTENIDO

0.-INTRODUCCION

Con los avances en Internet y los desarrollos de la informática y las telecomunicaciones, la Seguridad Informática, se ha convertido en figura necesaria para la protección, mantenimiento, control de acceso, confidencialidad, integridad y disponibilidad de la información, tanto para su seguridad como para la seguridad en el soporte de las operaciones de las organizaciones.

Las Políticas de Seguridad Informática son las directrices de índole técnica y de organización que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la información en él contenida. El principio y final de toda red es el usuario, esto hace que las políticasde seguridad deban, principalmente, enfocarse a los usuarios, estas indican a las personas cómo actuar frente a los recursos informáticos de la Entidad.

Actualmente la Contraloría Distrital de Buenaventura cuenta con una plataforma tecnológica que almacena, procesa y transmite la información institucional, la cual incluye equipos de cómputo de usuario y tres servidores que se interconectan por medio de una red de datos, así como servicio de internet y correo electrónico institucional. Siendo la información institucional un activo valioso para la Entidad, se hace necesario no solo la implementación de herramientas de hardware y software de seguridad, sino involucrar al personal para proteger su integridad y confidencialidad.

Este compendio tiene como finalidad dar a conocer las PSI - Políticas de Seguridad Informática, que deben aplicar y acatar los empleados, contratistas y terceros de la Contraloría Distrital de Buenaventura, entendiendo como premisa que la responsabilidad por la seguridad de la información es un compromiso de cada uno y en general de todos.

1.- OBJETIVO

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 Contraloría Distrital de Buenaventura, para su interiorización, aplicación y verificación permanente.

2.- ALCANCE

Las políticas de seguridad informática, están orientadas a todos los procesos informáticos y a la información almacenada, procesada y transmitida en medios electrónicos, estas políticas deben ser conocidas y cumplidas tanto por funcionarios de planta como por los contratistas que apoyan la gestión y por los terceros o grupos de interés que utilicen la información generada y custodiada por la Contraloría Distrital de Buenaventura, y por quienes hagan uso de los servicios tecnológicos de la Entidad.

3.- DEFINICIONES

Para los efectos del presente manual, se adoptarán las siguientes 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.

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.

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.

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.

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.

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.

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. En la Contraloría Distrital de Buenaventura se hace uso de la Herramienta Microsoft Office.

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 deredes sociales, formularios electrónicos, bases de datos, entre otros.

Integridad: propiedad de salvaguardar la exactitud y estado completo de losactivos.

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 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.

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.

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, CompactFlash, 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.

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: Posibilidad de que se produzca un contratiempo o una desgracia, las vulnerabilidades y amenazas a que se encuentran expuestos los activos de información.

Servicio informático: Conjunto de actividades asociadas al manejo automatizado de la información que satisfacen las necesidades de los usuarios.

Servidor: Se entiende como el software que configura un PC como servidor para facilitar el acceso a la red y sus recursos. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los clientes usualmente se conectan al servidor a través de la red, pero también pueden acceder

a él a través de la computadora donde está funcionando.

Sistema de información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

Software antivirus: Son programas que buscan prevenir, detectar y eliminar virus informáticos. En los últimos años, y debido a la expansión de Internet, los nuevos navegadores y el uso de ingeniería social, los antivirus han evolucionado para detectar varios tipos de software fraudulento, también conocidos como malware.

Software de gestión: Son todos aquellos programas utilizados a nivel empresarial, que por su definición genera acción de emprender algo y por su aplicación persigue fines lucrativo y no lucrativo. También es un software que permite gestionar todos los procesos de un negocio o de una empresa en forma integrada. Por lo general está compuesto por modulo cruzado de los procesos del negocio.

Software malicioso: Es aquel que se ha diseñado específicamente para dañar un computador, este tipo de software realiza acciones maliciosas como instalar software sin el consentimiento del usuario o virus.

Tráfico de red: Es la cantidad de datos enviados y recibidos por los usuarios de la red.

UPS: Sistema de alimentación ininterrumpida (SAI), en inglés uninterruptible power supply (UPS), es un dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.

4.- NORMATIVIDAD

Documentos de fundamentación Legal:

Ley 87 de 1993: “Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones”.

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

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

Ley 594 de 2000: “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.

Ley 599 de 2000: “Por la cual se expide el Código Penal”.

Ley 1437 de 2011: “Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo”.

Decreto 2609 de 2012: “Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado”.

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

Ley 2080 del 2021: Define el expediente electrónico, reglamentación y características.

Ley 2052 del 2020: Ordena la implementación de los servicios ciudadanos digitales.

Resolución 2893 del 2020: Define que el portal web debe constituirse en la sede electrónica de cada entidad; e integrarse al portal único del estado.

Resolución 1519 del 2021: Determina los estándares y directrices para publicar la información señalada en la ley de transparencia 1712 del 2014, y define que, los requisitos en materia de estándares de publicación y divulgación de contenidos, las condiciones de seguridad digital y los requisitos de datos abiertos.

5. POLÍTICAS GENERALES DE SEGURIDAD FISICA

a. Se destinará un área en la Enditad que servirá como centro de telecomunicaciones en el cual se ubicarán los sistemas de telecomunicaciones y servidores, debidamente protegidos con la infraestructura apropiada, de manera que se restrinja el acceso directo a usuarios no autorizados.

b. El centro de Telecomunicaciones deberá contar con sistema de protección contra incendios, control de temperatura (aire acondicionado) permanente a una temperatura no superior a 22 grados centígrados, así como sistema eléctrico de respaldo (UPS).

c. Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.

d. Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

e. Contar por lo menos con dos extintores de incendio adecuado y cercano al centro de telecomunicaciones.

f. Los equipos que hacen parte de la infraestructura tecnológica de la Contraloría Distrital de Buenaventura, tales como servidores, estaciones de trabajo, centro de cableado, UPS, dispositivos de almacenamiento, entre otros, deben estar protegidos y ubicados en sitios libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo.

6.- POLÍTICAS ORIENTADAS A LOS USUARIOS INTERNOS

6.1. Gestión de la Información:

a. Todo funcionario de planta o contratista que inicie labores en la Contraloría Distrital de Buenaventura, relacionadas con el uso de equipos de cómputo, software de gestión, aplicativos, plataformas web y servicios informáticos, debe aceptar las condiciones de confidencialidad y de uso adecuado de los recursos informáticos, así como cumplir y respetar las directrices impartidas en el Manual de Políticas de Seguridad Informática.

b. Los funcionarios que se desvinculen y los contratistas que culminen su vínculo contractual con la Contraloría Distrital de Buenaventura, deberán hacer entrega formal de los equipos asignados, así como de la totalidad de la información electrónica que se produjo y se recibió con motivo de sus funciones y actividades, como requisito para expedición de paz y salvo y/o liquidación de contrato.

c. Toda la información recibida y producida en el ejercicio de las funciones y cumplimiento de obligaciones contractuales, que se encuentre almacenada en los equipos de cómputo, pertenece a la Contraloría Distrital de Buenaventura, por lo tanto no se hará divulgación ni extracción de la misma sin previa autorización de las directivas de la Entidad.

d. No se realizará por parte de los funcionarios o contratistas copia no autorizada de información electrónica confidencial y software de propiedad de la Contraloría Distrital de Buenaventura. El retiro de información electrónica perteneciente a la Contraloría Distrital de Buenaventura y clasificada como confidencial, se hará única y exclusivamente con la autorización del Directivo competente.

e. Ningún funcionario o contratista podrá visualizar, copiar, alterar o destruir información que no se encuentre bajo su custodia.

f. Todo contrato o convenio relacionado con servicios de tecnología y/o acceso a información, debe contener una obligación o cláusula donde el contratista o tercero acepte el conocimiento de las políticas de seguridad y acuerde mantener confidencialidad de la información con la suscripción de un acuerdo o compromiso de confidencialidad de la información, el cual se hará extensivo a todos sus colaboradores.

6.2. Hardware y Software:

a. La instalación y desinstalación de software, la configuración lógica, conexión a red, instalación y desinstalación de dispositivos, la manipulación interna y reubicación de equipos de cómputo y periféricos, será realizada únicamente por personal del área del proceso tecnológico.

b. El espacio en disco duro de los equipos de cómputo pertenecientes a la Contraloría Distrital de Buenaventura será ocupado únicamente con información institucional, no se hará uso de ellos para almacenar información de tipo personal (documentos, imágenes, música, video).

c. Ningún funcionario o contratista podrá acceder a equipos de cómputo diferentes al suyo sin el consentimiento explícito de la persona responsable.

d. Ningún funcionario o contratista podrá interceptar datos informáticos en su origen, destino o en el interior de un sistema informático protegido o no con una medida de seguridad, sin autorización.

e. Ningún funcionario o contratista podrá impedir u obstaculizar el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, salvo el personal autorizado del área del proceso tecnológico en aplicación de las políticas o medidas de seguridad.

f. No se permite el uso de la plataforma y servicios informáticos (equipos de cómputo, periféricos, dispositivos, internet, red de datos, correo electrónico institucional) de la Contraloría Distrital de Buenaventura, para actividades que no estén relacionadas con las labores propias de La Entidad.

g. Los funcionarios y contratistas serán responsables de contar con los conocimientos actualizados en informática básica y el uso de herramientas ofimáticas.

6.3. Correo Electrónico:

a. El correo electrónico institucional es exclusivo para envío y recepción de mensajes de datos relacionados con las actividades de la Contraloría Distrital de Buenaventura, no se hará uso de él para fines personales como registros en redes sociales, registros en sitios web con actividades particulares o comerciales o en general entablar comunicaciones en asuntos no relacionados con las funciones y actividades en la Entidad.

b. La información transmitida a través de las cuentas de correo electrónico institucional no se considera correspondencia privada, ya que estas tienen como fin primordial la transmisión de información relacionada con las actividades ordinarias de la Contraloría Distrital de Buenaventura.

c. Es prohibido utilizar el correo electrónico institucional para divulgar información confidencial, reenviar mensajes que falten al respeto o atenten contra la dignidad e intimidad de las personas, difundir propaganda política, comercial, religiosa, racista, sexista o similares, reenviar contenido y anexos que atenten contra la propiedad intelectual.

d. Es responsabilidad del funcionario o contratista depurar su cuenta de correo institucional periódicamente, en todo caso se debe hacer copia de seguridad completa de los correos tanto recibidos como enviados.

6.4. Internet:

a. No se harán descargas de archivos por internet que no provengan de páginas conocidas o relacionadas con las funciones y actividades en la Entidad.

b. El Servicio de internet de la Contraloría Distrital de Buenaventura no podrá ser usado para fines diferentes a los requeridos en el desarrollo de las actividades misionales propias de la Entidad. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales, música, videos de YouTube y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

c. No es permitido el uso de Internet para actividades ilegales o que atenten contra la ética y el buen nombre de la Contraloría Distrital de Buenaventura o de las

personas.

d. La Contraloría Distrital de Buenaventura se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet de la Entidad.

6.5. Cuentas de Acceso:

a. Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles, cada funcionario y contratista es responsable por las cuentas de acceso asignadas y las transacciones que con ellas se realicen. Se permite su uso única y exclusivamente durante el tiempo que tenga vínculo laboral o contractual con la Contraloría Distrital de Buenaventura.

b. Las contraseñas de acceso deben poseer un mínimo de ocho (8) caracteres y debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (+-*/@#$%&). No debe contener vocales tildadas, ni eñes, ni espacios.

c. La contraseña inicial de acceso a la red que le sea asignada debe ser cambiada la primera vez que acceda al sistema, además, debe ser cambiada mínimo cada 4 meses, o cuando se considere necesario debido a alguna vulnerabilidad en los criterios de seguridad.

d. Solamente puede solicitar cambio o restablecimiento de contraseña el funcionario o contratista al cual pertenece dicho usuario, o el jefe inmediato mediante solicitud motivada al correo electrónico del área del proceso tecnológico.

e. Todo funcionario o contratista que se retire de la Entidad de forma definitiva o temporal (superior a 1 semana), deberá hacer entrega formal a quien lo reemplace en sus funciones o a su superior inmediato de las claves de acceso de las cuentas asignadas, con el fin de garantizar la continuidad de las operaciones a su cargo.

6.6. Seguridad Física:

a. Es responsabilidad de los funcionarios y contratistas velar por la conservación física de los equipos a ellos asignados, haciendo uso adecuado de ellos y en el caso de los equipos portátiles, estos podrán ser retirados de las instalaciones de la

Entidad única y exclusivamente por el usuario a cargo y estrictamente para ejercer labores que estén relacionadas con la Contraloría Distrital de Buenaventura. En caso de daño, pérdida o robo, se establecerá su responsabilidad a través de los procedimientos definidos por la normatividad para tal fin.

b. Los funcionarios y contratistas deberán reportar de forma inmediata a los directivos la detección de riesgos reales o potenciales sobre equipos de cómputo o de comunicaciones, tales como derrames de agua, choques eléctricos, caídas o golpes, peligro de incendio, peligro de robo, entre otros. Así como reportar de algún problema o violación de la seguridad de la información, del cual fueren testigos.

c. Mientras se operan equipos de cómputo, no se deberá consumir alimentos ni ingerir bebidas.

d. Se debe evitar colocar objetos encima de los equipos de cómputo que obstruyan las salidas de ventilación del monitor o de la CPU.

6.7. Derechos de Autor:

a. Ningún usuario, debe descargar y/o utilizar información, archivos, imagen, sonido, software u otros que estén protegidos por derechos de autor de terceros sin la previa autorización de los mismos.

6.8. Uso de Unidades de Almacenamiento Extraíbles:

a. Los funcionarios y contratistas que tengan información de propiedad de la Contraloría Distrital de Buenaventura en medios de almacenamiento removibles, deben protegerlos del acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

b. Toda información que provenga de un archivo externo de la Entidad o que deba ser restaurado tiene que ser analizado con el antivirus institucional vigente.

6.9. Clasificación de la información:

a. Los documentos electrónicos resultantes de los procesos misionales y de apoyo de la Contraloría Distrital de Buenaventura, se tratarán conforme a los lineamientos y parámetros establecidos en el Sistema de Gestión Documental de la entidad. Los activos de información asociados a cada sistema de información, serán identificados y clasificados por su tipo y uso siguiendo lo establecido en las tablas de retención documental vigentes.

6.10. Personal de sistemas:

a. El control de los equipos tecnológicos deberá estar bajo la responsabilidad del área del proceso tecnológico, así como la asignación de usuarios y la ubicación física.

b. En el área del proceso tecnológico se deberá llevar un control total y sistematizado de los recursos tecnológicos tanto de hardware como de software.

c. El área del proceso tecnológico y cada usuario del sistema, será la encargada de velar por que se cumpla con la normatividad vigente sobre propiedad intelectual de soporte lógico (software).

d. Las licencias de uso de software estarán bajo custodia del área del proceso tecnológico. Así mismo, los manuales y los medios de almacenamiento (CD, cintas magnéticas u otros medios) que acompañen a las versiones originales de software.

e. El área del proceso tecnológico es la única dependencia autorizada para realizar copia de seguridad del software original, aplicando los respectivos controles. Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

f. Todas las publicaciones que se realicen en el sitio WEB de la entidad, deberán atender el cumplimiento de las normas en materia de propiedad intelectual.

g. El acceso a los sistemas de información y red de datos será controlado por medio de nombres de usuario personales y contraseña. El área del proceso tecnológico será la encargada de crear y asignar las cuentas de acceso y sus permisos,

sistemas de información y correo electrónico, previo cumplimiento del procedimiento establecido para tal fin.

h. Las cuentas de acceso a sistemas, servicios y aplicaciones no podrán ser eliminadas al retiro de los funcionarios o contratistas, debe aplicarse la inactivación del usuario.

i. Se realizará backup a la información institucional y bases de datos, conforme a lo establecido en la política de backup y cronograma, así como en los casos extraordinarios: desvinculación de funcionario o contratista, envío de equipo para garantía, mantenimiento correctivo de equipo.

j. Las contraseñas de los usuarios administradores de las plataformas tecnológicas y sistemas de información de la entidad, deberán ser salvaguardadas por el área del proceso tecnológico.

k. La red interna de la Contraloría Distrital de Buenaventura deberá estar protegida de amenazas externas, a través de sistemas que permitan implementar reglas de control de tráfico desde y hacia la red.

l. Todos los equipos de la entidad, con OS Windows, deben tener instalado un antivirus, en funcionamiento, actualizado y debidamente licenciado.

m. Se realizará mantenimiento físico y lógico preventivo a los equipos de cómputo mínimo cada 6 meses, se deberá incluir el cableado estructurado. El área del proceso tecnológico deberá informar a la dirección administrativa, el requerimiento para la realización de los mantenimientos.

6.11. Directivos:

a. La Entidad debe garantizar capacitación a los funcionarios en el manejo del software de gestión, plataformas y aplicativos implementados en la Contraloría Distrital de Buenaventura.

b. Deberá notificarse al área del proceso tecnológico las novedades de vinculación y desvinculación de personal de la Contraloría Distrital de Buenaventura, con el fin de crear o cancelar, según sea el caso, los accesos a los sistemas de información, correo electrónico y red de datos.

7. POLÍTICAS ORIENTADAS A LOS USUARIOS EXTERNOS

a. El acceso de terceras personas a la Entidad debe ser controlado y su ingresoa las diferentes dependencias debe ser autorizado por los funcionarios a cargo.

8. POLÍTICA DE ADMINISTRACIÓN DE BACKUP

8.1. Objetivo

Establecer las directrices para la ejecución y control de las copias de seguridad de la información digital perteneciente a la Contraloría Distrital de Buenaventura.

8.2. Alcance

Estas directrices son aplicables a la información institucional, bases de datos y archivos de restauración de los equipos pertenecientes a la Contraloría Distrital de Buenaventura.

8.3. Clasificación de la Información

Información Institucional:
Entiéndase como información institucional aquella relativa a las operaciones realizadas por cada una de las dependencias de la Contraloría Distrital de Buenaventura, su producción, almacenamiento y gestión está a cargo de cada uno de los funcionarios y contratistas. Información que se encuentra alojada en los equipos de cómputo.

Bases de Datos:
Las bases de datos son el conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

8.4. Periodicidad del Backup

Tipo de Información	Frecuencia de Copia
Información Institucional	Una vez por semana
Bases de Datos	Tres veces por semana

8.5. Medios de Almacenamiento

Las copias de seguridad son almacenadas en un Disco Duro extraíble dispuesto exclusivamente para este fin. Este debe ser resguardado por el responsable del área del proceso tecnológico, acorde a las condiciones de seguridad brindadas por la entidad al área del proceso tecnológico.

8.6. Control de los Backups

Se debe llevar registro digital documentado de cada copia de seguridad realizada, de tal forma que se genere un expediente que permita el control de las copias realizadas y facilite la restauración de la información en caso de desastre.

8.7. Tipos de Backup

Las copias de seguridad se realizarán bajo el método de backup completo o en su defecto se podrá aplicar el método de backup completo y backup incremental.

Backup completo: se hace un respaldo completo de todos archivos del equipo. El backup abarca el 100% de los datos.

Backup incremental: se hace una copia de todos los archivos que han sido modificados desde que fue ejecutado el último backup completo.

8.8. Cronograma de Backups Información Institucional

Los usuarios deberán copiar su información al servidor acorde al procedimiento de Backups, y el proceso tecnológico realizará copia general de la información los días viernes de cada semana.

9. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL SITIO WEB

El sitio web de la Contraloría Distrital de Buenaventura (CDB) tiene como función principal proveer información y servicios, así como divulgar y promover normas y directrices internas y del Gobierno Nacional relacionadas con su objeto.

Conforme a los lineamientos de la Estrategia de Gobierno en Línea, la CDB publica los temas y actividades que tienen que ver con su misión, visión, objetivos y funciones por medio de su página www.contraloriabuenaventura.gov.co, informando sobre: trámites, servicios, indicadores de gestión, planes y programas, publicaciones, normas, convocatorias, información presupuestal, enlaces institucionales y, en general, información relacionada con el Proceso de Control Fiscal municipal.

La CDB solicita al visitante y al usuario de esta página que lea detalladamente estas condiciones y la política de privacidad, antes de iniciar su exploración o utilización. Si no está de acuerdo con estas condiciones de uso, le sugerimos que se abstenga de acceder o navegar por la página web de nuestra entidad.

Así mismo, es importante aclarar que la CDB no persigue ningún lucro, ganancia o interés comercial con los contenidos o vínculos que se publican en su página web www.contraloriabuenaventura.gov.co,

9.1 Aceptación de Términos

Cuando un usuario accede al sitio web de la CDB lo hace bajo su total responsabilidad y que, por tanto, acepta plenamente y sin reservas el contenido de los siguientes términos y condiciones de uso del sitio web de la entidad.

Esta declaración de uso adecuado de la información está sujeta a los términos y condiciones de la página web de la CDB, con lo cual constituye un acuerdo legal entre el usuario y la página de la CDB.

Si el usuario utiliza los servicios de la página web de la CDB, significa que ha leído, entendido y aceptado los términos expuestos. Si no está de acuerdo con ellos, tiene la opción de no proporcionar ninguna información personal, o no utilizar el servicio de la página web de la CDB, www.contraloriabuenaventura.gov.co,

9.2 Condiciones generales respecto al contenido del sitio web

a. La CDB se reserva, en todos los sentidos, el derecho de actualizar y modificar en cualquier momento y de cualquier forma, de manera unilateral y sin previo aviso, las presentes condiciones de uso y los contenidos de la página web www.contraloriabuenaventura.gov.co.

b. El sitio web tiene por finalidad brindar al usuario todo tipo de información relacionada con la gestión de la Contraloría Distrital de Buenaventura. La información contenida en esta página web, está redactada de forma breve, sencilla y clara, en formato de contenidos para web. La CDB procurará que la información satisfaga las necesidades de los usuarios.

c. El sitio web puede tener enlaces a otros sitios de interés o a documentos localizados en otras páginas web de propiedad de otras entidades, personas u organizaciones diferentes a la CDB. En estos casos el usuario deberá someterse a las condiciones de uso y a la política de privacidad de las respectivas páginas web.

d. La CDB no se hace responsable respecto a la información que se halle fuera de este sitio web y no sea gestionada directamente por el administrador del sitio web www.contraloriabuenaventura.gov.co,

e. Los vínculos (links) que aparecen en el sitio web tienen como propósito informar al usuario sobre la existencia de otras fuentes susceptibles de ampliar los contenidos que ofrece la página web o que guardan relación con ellos.

f. La CDB no garantiza ni se responsabiliza del funcionamiento o accesibilidad de las páginas web vinculadas. Tampoco sugiere, invita o recomienda la visita a las mismas. Por eso, no será responsable del resultado obtenido.

g. El establecimiento de un vínculo (link) con el sitio web de otra empresa, entidad o programa no implica necesariamente la existencia de relaciones entre la CDB y el propietario del sitio o página web vinculada, ni la aceptación o aprobación por parte de la CDB de sus contenidos o servicios.

h. Al ubicar en un sitio web el vínculo (link) de la página de la CDB, se deberá asegurar que direccione a la página de inicio.

i. Las personas que usen el vínculo (link) de la página de la CDB, deberán abstenerse de realizar manifestaciones o indicaciones falsas, inexactas o incorrectas sobre la CDB o incluir contenidos ilícitos, o contrarios a las buenas costumbres y al orden público.

j. Las investigaciones publicadas en la página web de la CDB no implican, de parte de la Entidad, juicio alguno o comprometen la posición de la entidad y/o de quienes intervienen en ella. Los contenidos son responsabilidad de quienes realizaron la investigación.

k. La prestación del servicio del sitio web de la CDB es de carácter libre y gratuito para los usuarios y se rige por los términos y condiciones que aquí se incluyen, los cuales se entienden como conocidos y aceptados por los (las) usuarios (as) del sitio.

9.3. Derechos de autor de los contenidos de la página web - Copyright

Este sitio de internet y su contenido son de propiedad intelectual de la CDB. Es posible descargar material de www.contraloriabuenaventura.gov.co, para uso personal y no comercial, siempre y cuando se haga expresa mención de la propiedad en cabeza de la CDB.

Respecto a los contenidos que aparecen en el sitio web de la CDB, el usuario se obliga a:

a. Usar los contenidos de forma diligente, correcta y lícita.

b. No suprimir, eludir, o manipular el copyright (derechos de autor) y demás datos que identifican los derechos de la CDB.

c. No emplear los contenidos y en particular la información de cualquier otra clase obtenida a través de la CDB o de los servicios, para emitir publicidad.

d. La CDB no será responsable por el uso indebido que hagan los usuarios del contenido de su sitio web.

e. El visitante o usuario del sitio web se hará responsable por cualquier uso indebido, ilícito o anormal que haga de los contenidos, información o servicios del sitio de la

CDB. El visitante o usuario del sitio, directa o por interpuesta persona, no atentará de ninguna manera contra el sitio web de la CDB, contra su plataforma tecnológica, contra sus sistemas de información ni tampoco interferirá en su normal funcionamiento.

f. El visitante o el usuario del sitio no alterará, bloqueará o realizará cualquier otro acto que impida mostrar o acceder a cualquier contenido, información o servicios del sitio web de la CDB, o que estén incorporados en las páginas web vinculadas.

g. El visitante o el usuario del sitio web de la CDB no enviará o transmitirá en este sitio o hacia el mismo a otros usuarios o a cualquier persona cualquier información de alcance obsceno, difamatorio, injuriante, calumniante o discriminatorio.

h. El visitante o el usuario del sitio web de la CDB no incurrirá en y desde el mismo en conductas ilícitas, como daños o ataques informáticos, interceptación de comunicaciones, infracciones a los derechos de autor, uso no autorizado de terminales, usurpación de identidad, revelación de secretos o falsedad en los documentos.

9.4. Ley Aplicable y Jurisdicción

El usuario no podrá manifestar ante la CDB o ante una autoridad judicial o administrativa, la aplicación de condición, norma o convenio que no esté expresamente incorporado en las presentes condiciones de uso.

Estas condiciones serán gobernadas por las leyes de la República de Colombia, en los aspectos que no estén expresamente regulados en ellas.

Si cualquier disposición de estas condiciones pierde validez o fuerza obligatoria, por cualquier razón, todas las demás disposiciones, conservan su fuerza obligatoria, carácter vinculante y generarán todos sus efectos.

Para cualquier efecto legal o judicial, el lugar de las presentes condiciones es el Distrito de Buenaventura, Departamento del Valle del Cauca, República de Colombia, y cualquier controversia que surja de su interpretación o aplicación se someterá a los jueces de la República de Colombia.

9.5. Duración y terminación

La prestación del servicio del sitio WEB de la CDB tiene una duración indefinida. Sin embargo, la entidad podrá dar por terminada o suspender la prestación de este servicio en cualquier momento. En caso de que se llegue a presentar esta situación, la CDB informará previamente sobre el hecho, para evitar mayores traumatismos.

9.6. Contáctenos

Si el usuario desea hacer sugerencias a la CDB para mejorar los contenidos, la información y los servicios que se ofrecen en el sitio web www.contraloriabuenaventura.gov.co, debe dirigirse al administrador de la página, en el siguiente correo electrónico: administrador@contraloriabuenaventura.gov.co.

10. CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

El Contralor Municipal, los jefes de Oficina o Procesos, el área del proceso tecnológico, los supervisores de contrato y el personal de la entidad, son responsables de conocer y asegurar la implementación de las políticas de seguridad informática, dentro de sus áreas de responsabilidad, así como del cumplimiento de las políticas por parte de su equipo de trabajo.

Elaboro: WILLIAN TENORIO ANGULO. - Profesional Universitario Sistemas
Reviso: WASHINGTON GONZALEZ CAICEDO. - Jefe Oficina Planeación