
	POLITICAS DE SEGURIDAD INFORMATICA	CODIGO: 30-24.04	VERSIÓN: 02
			PÁGINA 1 de 10

**POLITICAS DE USO DE SERVICIOS, RECURSOS INFORMATICOS,
TELECOMUNICACIONES Y SEGURIDAD DE LA INFORMACIÓN**

**CONTRALORA DISTRITAL DE BUENAVENTURA
CARMEN LORENA ASPRILLA QUEZADA**


**DIRECCIÓN OPERATIVA DE CONTROL FISCAL
JAIR PANAMEÑO VALENCIA
WILLIAN TENORIO ANGULO**

**CONTRALORIA DISTRITAL DE BUENAVENTURA
04 DE ENERO DEL 2016**

	POLITICAS DE SEGURIDAD INFORMATICA	CODIGO: 30-24.04	VERSIÓN: 02
			PÁGINA 2 de 10

CONTENIDO

	Pagina
INTRODUCCIÓN	3
1. POLITICA DE USO DE CUENTAS DE USUARIOS	4
2. POLITICA DE USO DE INTERNET	5
3. POLITICA DE USOS DE CORREO ELECTRONICO	6
4. POLITICA DE USO LA INTRANET	8
5. POLITICA DE USOS DE COMPUTADORES, IMPRESORAS Y PERIFERICOS	9
6. OTRAS POLITICAS	10

	POLITICAS DE SEGURIDAD INFORMATICA	CODIGO: 30-24.04	VERSIÓN: 02
			PÁGINA 3 de 10

INTRODUCCION

Considerando que la Contraloría Distrital de Buenaventura, se encuentra en proceso de implementación del Sistema de Gestión de la Calidad, y teniendo en cuenta que a través del Proceso de Soporte Informático se propone Administrar, desarrollar y mantener en buen estado las TIC, garantizando el apoyo logístico para el buen desarrollo de la Gestión; se adoptan las siguientes políticas de seguridad informáticas en la entidad:

1. Cuentas de Usuarios
2. Internet
3. Correo Electrónico
4. Red Interna
5. Políticas de uso de computadores, impresoras y periféricos
6. Otras Políticas

Mucho se ha hablado de las mejores prácticas que debemos tener para resguardar nuestra organización con respecto al uso de los recursos informáticos, tales como el correo electrónico, redes y de internet.

Hay discusiones sobre confidencialidad, propiedad de la información transmitida en los mensajes, códigos de ética y privacidad del correo.


Se ha realizado un listado de pautas que se deben tener en cuenta para dar un uso adecuado a los recursos informáticos como (computadores, correo electrónico, red interna, internet) provisto por la Contraloría Distrital de Buenaventura.

La Dirección Administrativa será la encargada de velar, por la realización periódica de la auditoría al interior de la entidad de los equipos de cómputo y periféricos así como el software instalado.

El propósito de estas políticas es asegurar que los funcionarios utilicen correctamente los recursos tecnológicos que la empresa pone a su disposición para el excelente desarrollo de las funciones institucionales.

Dichas políticas son de obligatorio cumplimiento.

El funcionario que incumpla las políticas de seguridad informática, responderá por sus acciones o por los daños causados a la infraestructura tecnológica de la empresa, de conformidad con las leyes penales, fiscales y disciplinarias.

	POLITICAS DE SEGURIDAD INFORMATICA	CODIGO: 30-24.04	VERSIÓN: 02
			PÁGINA 4 de 10

1. Cuentas de Usuarios


Es la cuenta que constituye la principal vía de acceso a los sistemas de información que posee la empresa; estas cuentas aíslan al usuario del entorno, impidiendo que pueda dañar al sistema o a otros usuarios, y permitiendo a su vez que pueda personalizar su entorno sin que esto afecte a otros.

Cada persona que acceda al sistema debe tener una sola cuenta de usuario. Esto permite realizar seguimiento y control, evita que interfieran las configuraciones de distintos usuarios o acceder al buzón de correo de otro usuario.

Una cuenta de usuario asigna permisos o privilegios al usuario para acceder a los sistemas de información y desarrollará actividades dentro de ellas. Los privilegios asignados delimitan las actividades que el usuario puede desarrollar sobre los sistemas de información y la red de datos.

Procedimiento para la creación de cuentas nuevas:

- La solicitud de una nueva cuenta o el cambio de privilegios, deberá hacerse por escrito y ser debidamente autorizada por la Oficina de Sistemas.
- Cuando un usuario recibe una cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad informática y acepta sus responsabilidades con relación al uso de esa cuenta.
- No debe concederse una cuenta a personas que no sean funcionarios de la empresa, a menos que estén debidamente autorizados.
- Los usuarios deben ingresar al sistema mediante cuentas que indiquen claramente su identidad. Esto también incluye a los administradores del sistema.
- La Dirección administrativa financiera y de talento Humano debe reportar a los administradores del Sistema, los funcionarios que ingresan a laborar a la entidad y requieran de la creación de una cuenta o así mismo de los que cesan sus actividades y solicitar la desactivación de su cuenta.
- Los Privilegios especiales de borrar o depurar los archivos de otros usuarios, sólo se otorgan a los encargados de la administración en la oficina de Sistemas.

	POLITICAS DE SEGURIDAD INFORMATICA	CODIGO: 30-24.04	VERSIÓN: 02
			PÁGINA 5 de 10


- No se otorgará cuentas a técnicos de mantenimiento externos a la institución, ni permitir su acceso remoto, a menos que la Dirección Administrativa en conjunto con el Administrador del de sistema determine que es necesario. En todo caso, esta facilidad solo debe habilitarse por el lapso requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto).
- No se crearán cuentas anónimas o de invitado.

2. Internet

Internet es una herramienta poderosa cuyo uso autoriza la empresa en forma extraordinaria, mas debe ser debidamente estructurada, puesto que contiene ciertos peligros. Los hackers o piratas informáticos están constantemente intentando hallar nuevas vulnerabilidades que puedan ser explotadas. Se debe aplicar una política que procure brindar la debida seguridad al uso de la misma y realizar monitoreo constante, por lo que se debe tener en cuenta lo siguiente:

A continuación se describen las políticas adoptadas para el uso adecuado de este importante servicio en las Instalaciones de la Entidad:

- El acceso a internet en horas laborales (de (8:00 a 12:00 y de 2:00 a 6:00) es de uso solo laboral no personal, con el fin de no saturar el ancho de banda y así poder hacer buen uso del servicio.
- No acceder a páginas de entretenimiento, pornografía, de contenido ilícito que atenten contra la dignidad e integridad humana: aquellas que realizan apología del terrorismo, páginas con contenido xenófobo, racista etc. o que estén fuera del contexto laboral.
- En ningún caso descargar, recibir, ni compartir información en archivos adjuntos de dudosa procedencia, esto para evitar el ingreso de virus a los equipo de la entidad.
- No descargar programas, demos, tutoriales, que no sean de apoyo para el desarrollo de las tareas diarias de cada empleado. La descarga de ficheros, programas o documentos que contravengan las normas de la entidad sobre instalación de software

	POLITICAS DE SEGURIDAD INFORMATICA	CODIGO: 30-24.04	VERSIÓN: 02
			PÁGINA 6 de 10

y propiedad intelectual están prohibidas y son responsabilidad de cada usuario. Ningún usuario está autorizado para instalar software en su ordenador. El usuario que necesite algún programa específico para desarrollar su actividad laboral, deberá comunicarlo a la Dirección Administrativa la cual se encargará de realizar las operaciones oportunas.


- Los empleados de la Institución tendrán acceso solo a la información necesaria para el desarrollo de sus actividades.
- Ningún empleado debe instalar ningún programa para ver vídeos o emisoras de televisión vía Internet y de música. (Ares, REAL AUDIO, BWV, etc.).
- No debe usarse el Internet para realizar llamadas internacionales (Dialpad, skipe, ET2PHONE, FREEPHONE, etc.).

3. Correo electrónico


El correo electrónico institucional, es un privilegio y se debe utilizar de forma responsable. Su principal propósito es servir como herramienta para agilizar las comunicaciones oficiales que apoyen la gestión institucional de la empresa. Es de anotar que el correo electrónico institucional es un instrumento de comunicación de la empresa y los usuarios tienen la responsabilidad de utilizarlo de forma eficiente, eficaz, ética y de acuerdo con la ley y normas establecidas por la institución.

A continuación se relacionan las políticas:

- Utilizar el correo electrónico institucional como una herramienta de trabajo, y no como nuestra casilla personal de mensajes a amigos y familiares, para eso está el correo personal.
- No enviar archivos de gran tamaño a compañeros de oficina. Para eso existe la red.
- No facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas. Los usuarios deben conocer la diferencia de utilizar cuentas de correo electrónico institucionales y cuentas privadas ofrecidas por otros proveedores de servicios en Internet.
- No participar en la propagación de mensajes encadenados o participar en esquemas piramidales o similares.

	POLITICAS DE SEGURIDAD INFORMATICA	CODIGO: 30-24.04	VERSIÓN: 02
			PÁGINA 7 de 10

- No distribuir mensajes con contenidos impropios y/o lesivos a la moral.
- No enviar grandes cadenas de mensajes no adecuados en forma interna.
- Si se recibe un correo de origen desconocido, consulten inmediatamente con el personal administrativo del Sistema sobre su seguridad. Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos a correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloggers, gusanos, etc).
- Cuando se contesta un correo, evitar poner "Contestar a todos" a no ser que estemos absolutamente seguros que el mensaje puede ser recibido por todos" los intervinientes.
- El acceso a las cuentas personales debe ser mínimo (o ninguno) durante nuestra jornada laboral.
- Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben establecer una contraseña para poder utilizar su cuenta de correo, y esta contraseña la deben mantener en secreto para que su cuenta de correo no pueda ser utilizada por otra persona, el funcionario es totalmente responsable de cualquier infracción que se cometa con su cuenta de correo institucional.
- Cuando el usuario deje de usar su estación de trabajo deberá cerrar el software de correo electrónico, para evitar que otra persona use su cuenta de correo.
- Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben mantener en línea el software de correo electrónico (si lo tiene disponible todo el día), y activada la opción de avisar cuando llegue un nuevo mensaje, o conectarse al correo electrónico con la mayor frecuencia posible para leer sus mensajes.
- Se debe eliminar permanentemente los mensajes innecesarios.
- Se debe mantener los mensajes que se desea conservar, agrupándolos por temas en carpetas personales.
- Utilizar siempre el campo "asunto" a fin de resumir el tema del mensaje.
- Evite usar las opciones de confirmación de entrega y lectura, a menos que sea un mensaje muy importante, ya que la mayoría de las veces esto provoca demasiado tráfico en la red.

	POLITICAS DE SEGURIDAD INFORMATICA	CODIGO: 30-24.04	VERSIÓN: 02
			PÁGINA 8 de 10

- Evite enviar mensajes a listas globales, a menos que sea un asunto oficial que involucre a toda la institución.
- La Oficina de Sistemas determinará el tamaño máximo que deben tener los mensajes del correo electrónico institucional.
- Si se desea mantener un mensaje en forma permanente, éste debe almacenarse en carpetas personales.

4. Intranet

La unidad Z es una carpeta compartida para todos los empleados de la Institución solo de uso laboral (compartir y almacenar información solo pertinente a sus tareas), no para almacenar información personales.


Al servidor de la entidad donde se encuentra alojada toda la información contable, financiera de la base de datos Oracle de la Contraloría Distrital de Buenaventura se le realizara Backup todos los días.

Si guardó una información en la red y más adelante ya no es necesario tenerla allí, debe eliminarse y guardarla ya sea en el equipo, o en memorias cd etc. Para no mantener la red llena de cosas innecesarias.

No utilizar la red con fines propagandísticos o comerciales.

No modificar ni manipular archivos que se encuentren en la red que no sean de su propiedad.


No guardar en la red música, videos o demás archivos de uso personal ni material innecesario.

	POLITICAS DE SEGURIDAD INFORMATICA	CODIGO: 30-24.04	VERSIÓN: 02
			PÁGINA 9 de 10

5. Políticas de uso de computadores, impresoras y periféricos.

La infraestructura tecnológica: servidores, impresoras, UPS, escáner, lectoras y equipos en general; no puede ser utilizado en funciones diferentes a las institucionales.

- Los usuarios no pueden instalar, suprimir o modificar el software originalmente entregado en su computador.
- No se puede instalar ni conectar dispositivos o partes diferentes a las entregadas en los equipos.
- No se puede utilizar memorias USB de sitios externos a la empresa, sin la previa revisión del antivirus para control de circulación de virus.
- No es permitido destapar o retirar la tapa de los equipos.
- Los equipos, escáner, impresoras, lectoras y demás dispositivos, no podrán ser trasladados del sitio que se les asignó inicialmente, sin previa autorización de la Dirección Administrativa.
- Se debe garantizar la estabilidad y buen funcionamiento de las instalaciones eléctricas, asegurando que los equipos estén conectados a las instalaciones eléctricas apropiadas de corriente regulada, fase, neutro y polo a tierra.
- Es estrictamente obligatorio, informar oportunamente a la Dirección Administrativa la ocurrencia de novedades por problemas técnicos, eléctricos, de planta física, líneas telefónicas, recurso humano, o cualquiera otra, que altere la correcta funcionalidad de los procesos. El reporte de las novedades debe realizarse a la Gerencia de Informática tan pronto se presente el problema.
- Los equipos deben estar ubicados en sitios adecuados, evitando la exposición al sol, al polvo o zonas que generen electricidad estática.
- Los protectores de pantalla y tapiz de escritorio, serán establecidos por la Dirección Administrativa y deben ser homogéneos para todos los usuarios.
- Ningún funcionario, podrá formatear los discos duros de los computadores.
- Ningún funcionario podrá retirar o implementar partes sin la autorización de la Dirección Administrativa.

	POLITICAS DE SEGURIDAD INFORMATICA	CODIGO: 30-24.04	VERSIÓN: 02
			PÁGINA 10 de 10

6. Otras Políticas

A los equipos portátiles personales externos a la entidad, no se les brindará soporte de ninguna índole; ni de hardware o de software, porque no son responsabilidad de la entidad por ende el dueño debe hacerse cargo y responsable de su computador.

La dirección IP asignada a cada equipo debe ser conservada y no se debe cambiar porque esto ocasionaría conflictos de IP'S y esto alteraría la latencia en el flujo de la red.

No llenar el espacio de disco del equipo con música ni videos, ni información que no sea necesaria para el desarrollo de sus tareas con respecto a la entidad.

Todo funcionario responsable de equipos informáticos debe dejarlo apagado y desenchufado tanto al medio día como en la noche lo anterior para ahorrar recursos energéticos y contribuir a la conservación de los equipos.

“El correcto manejo de los equipos de sistemas de la empresa es responsabilidad directa de cada funcionario”.

ELABORO	APROBÓ	FECHA DE IMPLEMENTACIÓN
TECNICO OPERATIVO DE ONTROL FISCAL	CARMEN LORENA ASPRILLA QUEZADA CONTRALORA DISTRITAL DE BUENAVENTURA	31-MARZO-2014

Proyecto y Elaboro Jair Panameño Valencia