OBJETIVO

El presente documento tiene como finalidad dar a conocer las **Políticas y estándares de Seguridad Informática** que deberán prestar mucha atención los funcionarios cuando utilicen o soliciten un servicio al Área de Sistemas, para proteger adecuadamente los activos tecnológicos y la información almacenada en los diferentes dispositivos con los que cuenta la compañía.

Por este motivo es conveniente que cada uno de los funcionarios de la compañía lean y entiendan este documento para tener claro lo que aquí se menciona y de esta forma evitar malos entendidos en el uso de los servicios informáticos.

INTRODUCCIÓN

La Seguridad Informática, es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades de la compañía en materia de seguridad.

El hardware debe ser para uso exclusivo de la compañía, el uso indebido de los mismos puede acarrear sanciones administrativas y disciplinarias, como lo establece el manual de Políticas de Seguridad Informática, donde no puede ser alterada la configuración por ningún motivo, a no ser por autorización de las Directivas de la compañía o del Área de Sistemas.

La información debe ser almacenada en el servidor de archivos y no en los Discos locales del equipo de cómputo, de lo contrario no será respaldada de acuerdo a las políticas de respaldo que posee la compañía y no será responsabilidad del Área de Sistemas en caso contrario.

El manejo de las claves debe ser completamente confidencial e intransferible, donde se debe tener el cumplimiento de buenas prácticas de seguridad para tener un dominio de confidencialidad, disponibilidad e integridad de la información.

Tabla de contenido

CONFIDENCIALIDAD Y DERECHOS DE AUTOR

El Funcionario o empleado al momento de firmar contrato con la empresa acepta que todo aplicativo, programa, utilidad, documentación escrita o magnética, que haya realizado por sus funciones laborales u oficio es de propiedad de la compañía y no podrá sustraer, destruir ocultar, inutilizar, divulgar o alterar total o parcialmente y de manera indebida sin la autorización de la Gerencia General de Constructora Bolívar Cali S.A.

Al momento de ingresar a la empresa el Funcionario se compromete a respetar los Derechos de Autor en el cual no va reproducir, distribuir vender, arrendar o instalar, un programa o aplicativo (Software) sin la autorización de la empresa o autor dueña de la información.

Por razones de su oficio el Funcionario deberá custodiar y cuidar la documentación e información que por razones de sus labores, cargo u oficio, tenga bajo su responsabilidad e impedir o evitar su uso, sustracción destrucción, ocultamiento o inutilización indebidos.

En caso de incumplir algún de los preceptos mencionados arriba o lo indicado en este manual el Funcionario será sancionado disciplinariamente por la Empresa o penalmente si llegara a ser necesario como lo estipula la Ley en Colombia para proteger los Derechos de Autor.

POLÍTICAS EN LA ADMINISTRACIÓN DE LOS RECURSOS FÍSICOS

El acceso a áreas restringidas como son los Centros de cómputo, cuartos de comunicaciones o de suministro de energía UPS o planta eléctrica por parte de Funcionarios y proveedores, solo puede ser por personal previamente autorizado por el Área de Sistemas o Administrativa.

El Funcionario deberá reportar de forma inmediata al Área de Sistemas o Administrativa, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo, comunicaciones o cualquier otro elemento o equipo, como pueden ser fugas de agua, conatos de incendio u otros.

El Funcionario tiene la obligación de proteger los discos, disquetes, cintas magnéticas, CD-ROM, dispositivos de almacenamiento extraíbles USB o cualquier otro componente de almacenamiento que se encuentren bajo su administración, aún cuando no se utilicen y contengan información reservada o confidencial.

Es responsabilidad del Funcionario evitar en todo momento la fuga de la información de la Empresa que se encuentre almacenada en los equipos de cómputo personal o que tenga asignados.

Controles de acceso físico

Cualquier persona que tenga acceso a las instalaciones de la compañía, deberá registrar al momento de su entrada en la portería de la compañía, el equipo de cómputo, equipo de comunicaciones (tablets y Portátiles) y herramientas que no sean propiedad de Constructora Bolívar Cali S.A., podrán ser retirarlas el mismo día. En caso contrario deberá tramitar la autorización de salida respectiva con el Área de Sistemas y Administrativa.

Los computadores personales, computadores portátiles, impresoras o cualquier activo de cómputo propio o en arriendo, podrá salir de las instalaciones de la Empresa únicamente con la autorización de salida del Área de Sistemas y Administrativa de Constructora Bolívar Cali.

Seguridad en los sitios o áreas de trabajo

Los centros de cómputo de Constructora Bolivar Cali es área restringida, por lo que sólo el personal autorizado por el Área de Sistemas puede acceder a él.

Protección y ubicación de los equipos

Los Funcionarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Área de Sistemas, en caso de requerir este servicio deberá solicitarlo o solicitar autorización a estas mismas áreas.

El Área de Gestión Humana será la encargada de generar el resguardo y obtener la firma del Funcionario como responsable de los activos de cómputo asignados por la Empresa para su servicio.

Los Funcionarios deberán utilizar los mecanismos corporativos para proteger la información que reside y utiliza la infraestructura tecnológica de Constructora Bolívar Cali S.A. de igual forma, deberán proteger la información reservada o confidencial que por necesidades corporativas deba ser almacenada o transmitida, ya sea dentro de la red interna (LAN) o hacia redes externas como Internet (WAN).

Los Funcionarios de Constructora Bolívar Cali S.A. que hagan uso de los equipos de cómputos, deben conocer y aplicar las medidas para prevenir de código malicioso como pueden ser virus, caballos de Troya o gusanos de red para ello se ha instalado en los equipos de cómputo un software de antivirus. Para aquellos que tienen computadores portátiles deberán tener instalado un antivirus.

Uso de medios de almacenamiento

Para evitar perdida de información todos los Funcionarios deben almacenar la información en los servidores de archivos dispuestos para este fin, para esta acción debe autenticarse en el servidor utilizando la credencial entregada por el Área de Sistemas, de esta forma se asegura que la información almacenada en estos servidores será respaldada de acuerdo a los mecanismos adoptados por el Área de Sistemas, según los procedimientos de respaldos definidos.

Toda solicitud para utilizar un medio de almacenamiento de información compartida (Carpetas Compartidas), deberá contar con la autorización del área dueña de la información. El personal que requiera estos medios debe justificar su utilización. Dicha justificación deberá hacerla llegar al Área de Sistemas escrita o por correo electrónico por el Jefe del Área de adscripción.

En caso de que por la magnitud de información a respaldar se requiera algún CD o DVD, este último deberá solicitarse por escrito o correo electrónico al Área de Sistemas justificando la razón de la solicitud.

Las actividades que realicen los Funcionarios en los recursos informática de Constructora Bolívar Cali S.A. son registradas y susceptibles de auditoria en cualquier momento.

Mantenimiento de los equipos de cómputo

Este servicio únicamente lo realizara personal especializado el cual esta autorizado por el Área de Sistemas. La empresa prestadora del servicio podrá llevar a cabo la limpieza o reparación de los equipos de cómputo por lo que el Funcionario podrá solicitar la identificación del personal designado en caso de ser necesario.

Al momento de realizar el mantenimiento preventivo de los equipos el Funcionario debe respaldar o guardar la información para evitar perdida de esta o así mismo cuando el equipo de computo sea enviado para ser reparado, de esta manera se evita que en caso de daño de los medios de almacenamiento provistos en el equipo de computo se vean afectados involuntariamente en el procedimiento de reparación. Cuando el equipo es en arriendo se debe borrar la información almacenada en el equipo, en caso de ser retirado del sitio de trabajo para ser revisado en las instalaciones de la compañía arrendadora.

En el caso de los equipos en arriendo estos servicios lo realizara directamente la empresa prestadora del servicio, pero de igual forma debe tenerse en cuenta los puntos antes mencionados.

Cuando el equipo en arriendo sea devuelto a la compañía prestadora del servicio por termino del contrato o entrega unilateral de alguna de las dos partes, debe formatearse el disco duro para evitar que información sensible de la compañía llegue a manos de

terceros, en caso de requerir asistencia para esta acción se debe solicitar soporte al Área de Sistemas, la cual orientará en este procedimiento.

En caso de requerir un servicio de mantenimiento el Funcionario deberá solicitarlo ya sea por correo electrónico, telefónicamente o por escrito al Área de Sistemas para de esta manera realizar el procedimiento correspondiente para prestar la ayuda o servicio de acuerdo a la necesidad.

POLÍTICAS PARA LA ADMINISTRACIÓN DE LOS RECURSOS LÓGICOS

Instalación de Software

Se considera una falta grave que los Funcionarios instalen cualquier tipo de programa (software) en los computadores asignados, servidores o cualquier equipo conectado a la red de Constructora Bolívar Cali S.A., que no haya sido autorizado por el Área de Sistemas o la Gerencia General de la compañía e incurrirá en sanciones disciplinarias por parte de la empresa.

Identificación del incidente

El Funcionario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá notificarlo al Área de Sistemas lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las entidades administrativas competentes dentro de la compañía, el Funcionario deberá notificar a su Jefe o Gerente inmediato.

Cualquier incidente generado durante la utilización u operación de los activos de informática de Constructora Bolívar Cali S.A. debe ser reportado al Área de Sistemas.

Administración de la configuración

Los Funcionarios de Constructora Bolívar Cali S.A. no deben montar o configurar redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red Constructora Bolívar Cali S.A.

Seguridad para la red

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el Área de Sistemas, en la cual los Funcionarios realicen la exploración de los recursos informáticos en la red de la Constructora Bolívar Cali S.A., así como de los aplicativos que la compañía utiliza día a día para la gestión y desarrollo del negocio, con fines de detectar y explotar una posible vulnerabilidad.

Uso del Correo electrónico

Los Funcionarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el Funcionario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa que no sea del servidor de correos de la compañía.

Los Funcionarios deben manipular los mensajes de correo electrónico y archivos adjuntos como información de propiedad de Constructora Bolívar Cali S.A. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

Constructora Bolívar Cali S.A. se reserva el derecho a acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad, violado políticas de Seguridad Informática de la Empresa o realizado acciones no autorizadas.

El Funcionario debe de utilizar el correo electrónico de la Empresa única y exclusivamente para el desempeño de sus funciones, oficio o cargo, quedando prohibido cualquier otro uso que no sea de carácter laboral.

La creación de una cuenta de correo electrónico debe ser solicitada por el Área de Gestión Humana por medio de un correo electrónico.

Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un Funcionario de correo electrónico.

Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

El Funcionario deberá preservar en todo momento la utilización de un lenguaje apropiado, evitando palabras ofensivas o altisonantes.

Controles contra código malicioso

Para prevenir infecciones por virus informáticos, los usuarios de la compañía no deben hacer uso de software que no haya sido proporcionado y validado por el Área de Sistemas.

Los usuarios de la Empresa deben verificar que la información y los medios de almacenamiento, considerando al menos discos flexibles, CD's, cintas, cartuchos y dispositivos de almacenamiento extraíbles (USB), estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus instalado en los equipos de computo. Sí por algún motivo no es posible realizar esta labor, hacer llegar el medio de almacenamiento al Área de Sistemas para realizar la inspección del mismo y garantizar el uso posterior.

Todos los archivos que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos o cualquier tipo de documento de informática que tengan que ser descomprimidos, el Funcionario debe verificar que estén libres de virus utilizando el software antivirus instalado en el equipo de computo.

Ningún Funcionario de la Empresa debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código alguno diseñado para auto replicarse, dañar, o en otros casos impedir el funcionamiento del equipo de cómputo, sistema operativo o software de uso de la Empresa. Mucho menos probarlos en cualquiera de los ambientes o plataformas de la Empresa. El incumplimiento de lo anterior será considerado una falta grave y será sancionada disciplinariamente.

Ningún Funcionario, empleado o personal externo, podrá bajar o descargar software de sistemas, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del Área de Sistemas.

En caso de infección de virus en el equipo de cómputo el Funcionario deberá informar al Área de Sistemas inmediatamente par recibir las instrucciones o procedimiento a seguir para detectar y erradicar el virus o código malicioso.

Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la compañía en: Antivirus, Outlook, Microsoft Office, Navegadores o cualquier otro programa.

Uso del Servicio de Internet

El servicio de Internet provisto a los usuarios es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por Constructora Bolívar Cali S.A., en caso de necesitar una conexión a Internet especial o adicional, ésta tiene que ser notificada y aprobada por la Gerencia y/o persona autorizada por la misma.

Los Funcionarios con acceso al servicio de navegación serán sujetos de monitoreo de las actividades que realiza en Internet, no podrá acceder a páginas no autorizadas, que puedan vulnerar los sistemas de la compañía. Queda prohibido la transmisión de archivos reservados o confidenciales no autorizados y se prohíbe descargar software sin la autorización del Área de Sistemas. La utilización del Internet es para el desempeño de sus funciones y puesto en la Empresa y no para propósitos personales.

En caso de llegarse a comprobar un mal uso del servicio de Internet será suspendido inmediatamente, con notificación al Jefe inmediato y al área de Gestión Humana para que tomen las medidas disciplinarias pertinentes.

Control de acceso lógico

Cada Funcionario es responsable de la información de control de acceso que le sean proporcionados es decir, usuario y contraseña para acceder a los diferentes servicios, aplicativos y servidores de informática de Constructora Bolívar Cali S.A. y deberá mantener en absoluta confidencialidad.

Los permisos entregados al Funcionario serán de acuerdo al cargo que desempeñará dentro de la organización. En caso de requerir permisos adicionales o especiales deberán ser notificados al Área de Sistemas por correo electrónico del Director del área o Gerencia.

El Área de Gestión Humana enviará al área de Sistemas con copia al Director del área o Gerencia, por correo electrónico la notificación para crear las credenciales de acceso a los sistemas de información de los Funcionarios vinculados a la Empresa. De esta manera se creará, asignará los permisos a los aplicativos y recursos, de acuerdo al cargo que desempeñara el Funcionario dentro de la Empresa.

Controles de acceso

El acceso de personal externo a la infraestructura tecnológica de la Cía debe ser autorizado por un Director o Gerente de Constructora Bolívar Cali S.A., quien deberá notificar al Área de Sistemas para realizar los ajustes necesarios.

El Director o Gerente, deberá estar alerta para evitar que el personal externo al cual se le ha entregado autorización para utilizar los recursos informáticos de Constructora Bolívar Cali S.A., haga buen uso de los mismos y estar atento de que no se lleve información sensible para la organización, a no ser que haya sido autorizado por la Gerencia General o el dueño de dicha información.

Esta totalmente prohibido que los funcionarios utilicen los recursos informáticos de la compañía para obtener acceso no autorizado a recursos, carpetas o sistemas a los cuales no se le ha otorgado permisos o utilicen una cuenta de usuario sin autorización de este último para acceder a lo antes mencionado.

Los Funcionarios no deben proporcionar información de los sistemas, infraestructura, instalaciones de informática o computo a personal externo, a no ser que se tenga una autorización del Área de Sistemas o de las Directivas de la Empresa.

Cada Funcionario debe utilizar y tener la Cuenta de Usuario asignada para acceder a los sistemas de información de la compañía. Esta cuenta de usuario no puede ser utilizada por varios usuarios ni debe ser revelada la contraseña de la misma.

Los usuarios son responsables de todas las actividades realizadas con su Cuenta de usuario asignada. Los usuarios no deben divulgar ni permitir que otros utilicen sus identificaciones de usuario, al igual que tienen prohibido utilizar la Cuenta de Usuario de otros usuarios.

Los cambios y responsabilidades en las funciones de un Empleado que implique modificar los permisos asignados anteriormente deberán ser notificados mediante correo electrónico por el Área de Gestión Humana o del Director al Área de Sistemas para realizar el procedimiento respectivo.

Administración y uso de las cuentas de usuario

La asignación de las cuentas y contraseñas se harán de manera individual y particular por lo que ésta información es prohibida compartirla.

Si el Funcionario olvida, bloquea o extravía alguna de sus credenciales de ingreso a los recursos informáticos deberá informar al Área de Sistemas mediante correo electrónico del Funcionario o Director del area, para proporcionarle una nueva contraseña, luego de recibirla deberá ser modificada por el Funcionario.

Está prohibido que las contraseñas se encuentren en cualquier medio impreso o magnético y en lugares donde personas sin autorización puedan encontrarlas.

Es prohibido que las contraseñas sean reveladas o compartidas. En caso dado el Funcionario se responsabiliza por las acciones que le den a la misma en los recursos informáticos, pudiendo llegar a sanciones disciplinarias.

Se deben manejar los siguientes lineamientos para elaborar una contraseña en los diferentes recursos informáticos:

1. Debe estar compuesta mínimo por 10 caracteres alfanuméricos.
2. Debe contener letras mayúsculas y minúsculas
3. Debe contener al menos un carácter especial.
4. Las contraseñas no deben tener información personal ni laboral.
5. No deben utilizarse contraseñas anteriormente asignadas

Las contraseñas tendrán una vigencia de 90 días, después de este lapso debe ser cambiada por una nueva.

Cuando un funcionario crea que su contraseña haya sido revelada, debe realizar el cambio inmediatamente e informar al Área de Sistemas para que en conjunto se realice el cambio de la misma.

Cuando un Funcionario es relegado o suspendido de sus funciones, el Área de Gestión Humana o el Director del área, deberán hacerlo saber en el menor tiempo posible al Área de Sistemas para bloquear o suprimir las credenciales del Funcionario, mediante un correo electrónico la acción demandada.

Control de acceso remoto o locales

El encargado del área de Sistemas o la persona autorizada por el mismo, tiene permitido el acceso a equipos dentro de la red local o remota de otros Funcionarios, con fines de soporte, corrección, instalación o configuración de los equipos de cómputo, servidores o recursos informáticos.

Está totalmente prohibido que un Funcionario instale equipos de comunicaciones, programas de acceso remoto o cualquier dispositivo que permita la recepción remota en los equipo de computo, servidores o recursos informáticos de la empresa, sin la autorización del Área de Sistemas o la Gerencia General de la compañía. Si llega a realizarse esta acción el funcionario será sancionado disciplinariamente.

Uso de medios de almacenamiento

Los funcionarios deberán respaldar diariamente la información sensitiva y crítica que se encuentre en sus computadoras o estaciones de trabajo, en los servidores dispuestos para esta labor.

En caso de que por la magnitud de información a respaldar se requiera algún CD o DVD, este último deberá solicitarse por escrito o correo electrónico al Área de Sistemas justificando la razón de la solicitud.

Las actividades que realicen los Funcionarios en los recursos de informática de Constructora Bolívar Cali S.A. son registradas y susceptibles de auditoria en cualquier momento.

Yo_____identificado (a) con C.C._____recibí información del manual de políticas y seguridad de los recursos informáticos de Constructora Bolívar Cali con las recomendaciones del área de sistemas acerca del correcto uso de la información, manejo seguro de claves y escritura de correos electrónicos y me comprometo a seguir las normas establecidas por el área y acepto las sanciones pertinentes en caso de incumplirlas.

Por lo anterior, se firma en_____a los (_) días del mes de_____.

_____ _____

Nombre Firma