



# **POLITICA DE TECNOLOGIA DE INFORMACION Y COMUNICACIÓN**

## **POLITICA DE TECNOLOGIAS DE INFORMACION Y COMUNICACIÓN**

La evolución tecnológica ha llevado a las empresas a considerar que las tecnologías de información y comunicaciones desempeñan un rol estratégico en el mundo de los datos y que estos son información y conocimientos difíciles de asimilar por el ritmo que se generan.

Bajo este contexto es necesario considerar la vital importancia de la información procesada por los usuarios de los procesos de tecnología y aplicaciones de QBCo S.A. y que esta deba estar organizada bajo reglas claras, mediante las cuales se pueda garantizar la disponibilidad, integridad y la confiabilidad de la misma.

De igual forma sucede con las herramientas de apoyo y el software. El Internet y los sistemas de correo electrónico son herramientas de apoyo que ayudan a la consulta de información, comunicación rápida, administración de tareas, entre otros beneficios.

Por otro lado se encuentra el Software o Aplicaciones, que contribuyen a la creación, administración, operación y consulta de información de la Organización.

Concluyendo, es importante establecer políticas de seguridad de tecnologías de información y comunicaciones con la finalidad de salvaguardar la información y los bienes informáticos de QBCo S.A. , lo cual constituye uno de los activos más importantes de la organización.

## OBJETIVO

El Objetivo de este documento es establecer las políticas de seguridad de Tecnología de Información y Comunicaciones que deben conocer y cumplir todo colaborador de QBCo S.A. , estas se agrupan en:

- Políticas para el uso adecuado de las Tecnologías de Información y Comunicación
- Política de Contraseñas y Claves.
- Políticas de Internet y Correo Electrónico
- Políticas para el uso de Software.
- Políticas de Capacitación.

Estas reglas buscan proteger la información, a los colaboradores y a la empresa, buscando propiciar un aumento de la seguridad y aprovechamiento de la tecnología, la cual contribuirá de manera determinante a aumentar la eficiencia en el trabajo y garantizar la continuidad de las operaciones dentro de la Organización.

## **ALCANCE**

Estas políticas son aplicables y actualmente efectivas para todos los colaboradores que utilicen equipo de cómputo o herramientas tecnológicas ya sea de hardware o software que pertenezcan a la organización QBCo S.A ya sea de manera directa o suministrada a través de un tercero.

Los usuarios de QBCo S.A. tienen la obligación de tener presente estas políticas emitidas por la Gerencia de Tecnología y aprobadas por la Gerencia General.

La Gerencia de Tecnología es la encargada de administrar estas políticas.

Los equipos de cómputo regulados y atendidos por esta política son:

- El que es parte del Activo Fijo de QBCo S.A.
- El que se encuentra en modalidad de arrendamiento directo.
- El que se encuentra en modalidad de arrendamiento financiero.
- El Software adquirido de manera directa o licenciado a través de un tercero
- El Hardware adquirido de manera directa o a través de servicios prestados por terceros.

## CONSIDERACIONES GENERALES

### Uso Adecuado de la Tecnología de Información y Comunicaciones.

Las políticas definidas en este punto están relacionadas con los equipos de computo que les son asignados a los colaboradores de QBCo S.A., así como del software a que tiene acceso cada colaborador, aspectos relacionados con el Centro de Datos, como también temas relacionados con la propiedad de la información que es creada y trabajada por los colaboradores de QBCo S.A., e igualmente con la utilización inadecuada de los recursos informáticos que QBCo S.A. pone a disposición de sus colaboradores para que desarrollen sus actividades. Esta parte de la política constituye la base de las políticas que debe cumplir todas las personas que trabajan en QBCo S.A.

## Contraseñas y Claves:

El cumplimiento de las políticas de contraseñas y claves por parte de los colaboradores de QBCo S.A. , es extremadamente importante ya que estas constituyen la primera línea de defensa para garantizar que la información solo sea accedida por las personas autorizadas.

Tanto equipos, sistemas y datos utilizan mecanismos de contraseña para controlar el acceso, como es el caso de contraseñas para acceso a los equipos, para ingreso a la red de la organización, para utilizar sistemas, aplicaciones y software en general. No existe una tecnología que pueda prevenir el acceso no autorizado a la información, si un usuario viola esta política, de ahí que sea una de las más relevantes e importantes.

### Correo Electrónico e Internet:

Los accesos a Internet y Correo Electrónico son servicios que actualmente son utilizados por los colaboradores de QBCo S.A. con los siguientes beneficios:

- Interactuar de una forma directa, ágil y eficiente, a través de la mensajería electrónica con nuestros clientes y proveedores, con el ámbito institucional y gubernamental, así como dentro de las diferentes áreas y colaboradores de la Organización.
- Ofrecer a través de Internet una herramienta de Investigación que permita realizar consultas de cubrimiento nacional e internacional desde su sitio de trabajo.
- Ingresar a diferentes servicios ofrecidos por Organizaciones Públicas, Gubernamentales, Bancarias y Privadas que nos permiten optimizar procesos y tiempos de operación.

El internet y el correo electrónico se han convertido en medios de comunicación electrónicos prácticamente indispensables para el trabajo diario por lo que es muy importante cumplir con las políticas relacionadas con ellos.

De esa forma evitamos interrupciones que podrían afectar la productividad, imagen y metas de QBCo S.A.

## Uso de Software:

Las aplicaciones, desarrollos y programas conocidos de manera general como Software, están protegidos por las leyes de derecho de autor y por tratados internacionales, desafortunadamente algunas veces se ignora el hecho de que el software tiene un valor económico, sin embargo el software es un elemento crítico de varios aspectos de funcionamiento de la empresa y por lo tanto debe administrarse y debe tener políticas.

Las políticas sobre el uso del software en QBCo S.A., se crean para que sirvan de marco regulatorio en cuanto a la instalación y uso de software en el equipo de computo propiedad de QBCo S.A., y de los equipos bajo modalidad de arrendamiento directo, operacional o financiero.

## **POLÍTICA PARA EL USO ADECUADO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES**

### **GENERALES.**

- Bajo ninguna circunstancia los colaboradores de QBCo S.A., pueden utilizar los recursos informáticos para realizar actividades prohibidas por las normas internas establecidas en la organización o por normas jurídicas nacionales o internacionales.
- Para los equipos propiedad de QBCo S.A., El Área de Tecnología es la única autorizada a realizar las actividades de soporte técnico y cambios de configuración en el equipo de cómputo ya sea de manera directa o a través de terceros.
- En el caso de labores de Mantenimiento efectuadas por terceros, estas deben ser previamente aprobadas por la Gerencia de Tecnología.
- Para los equipos de cómputo en esquema de arrendamiento directo, la empresa arrendadora es la única autorizada a realizar las labores de mantenimiento y cambio de hardware o en su caso, autorizar la realización de dichas labores a un tercero.

## EQUIPO DE CÓMPUTO,

- El equipo de computo, propiedad de QBCo S.A. o arrendado bajo las diferentes modalidades, deberá ser utilizado únicamente para actividades relacionadas con los objetivos y metas de la empresa.
- Para el correcto funcionamiento del equipo deberán realizarse periódicamente y por lo menos una vez al año, mantenimientos preventivos que permitan la revisión de las condiciones físicas del equipo así como de la operación del mismo.
- La Asignación de los equipos deberá realizarse de manera coordinada entre la Gerencia de Tecnología y la Gerencia del Área a la cual el colaborador pertenece.
- La solicitud de mantenimiento de un equipo por daño o mal funcionamiento, deberá ser tramitada por el colaborador, informando al Área de Tecnología de la novedad que se presenta, igualmente la adquisición de accesorios adicionales deberá contar con la aprobación del Área de Tecnología y de la Gerencia del Área a la cual, el colaborador que realice la solicitud, pertenezca.
- El equipo de computo para la Empresa QBCo S.A. será establecida de manera standard en su configuración y accesorios, de acuerdo a la definición establecida por el Área de Tecnología, teniendo en cuenta los avances y propuestas existentes en el mercado. Cualquier cambio o requerimiento adicional solicitado al modelo standard establecido, deberá contar con la aprobación de la Gerencia de Tecnología y de la Gerencia del Área a la cual el colaborador que realice la solicitud, pertenezca.

Las características de los equipos definidos al día de hoy para los colaboradores de la Empresa QBCo S.A. son los siguientes:

Equipo Laptop Dell Inspiron 14": El cual posee la característica para ser usado por personas que no realizan desplazamientos constantes o por fuera de las instalaciones de la empresa.

Equipo Laptop Vostro 3360 : el cual posee las característica de ser menos pesado, por lo que se direccionaría para aquellos colaboradores que constantemente realizan desplazamientos fuera de las instalaciones de la empresa ( Vendedores y Gerencias ).

- Para conectar un computador a la red institucional que no este bajo el control administrativo de QBCo S.A., ( Computadores Privados, Computadores de Otras Empresas o Terceros en General, las cuales no están sujetas a la totalidad de la políticas de seguridad de QBCo S.A., y por ende constituyen un riesgo al ser conectadas a la red institucional ), se deberá solicitar permiso a la Gerencia de Tecnología para que esta inspeccione el equipo , compruebe que no constituye un riesgo para la seguridad de la información de la compañía, evalúe el porque de la necesidad de conectar el equipo a nuestra red privada y de la autorización en su caso.
- Cuando exista algún incidente (robo, extravió, venta, daño físico, etc), que afecte de manera directa a un equipo de computo de QBCo S.A., debe ser notificado de inmediato a la Gerencia de Tecnología y adicionalmente, para aquellos casos donde el equipo este bajo cualquier modalidad de arrendamiento, a la Gerencia Financiera para revisión de los temas de contrato y políticas de leasing.
- El reintegro del equipo incluido en un siniestro (robo, extravió, daño físico. Etc.) se debe realizar de acuerdo a las políticas establecidas por el área de recursos humanos acerca del manejo y preservación de los activos fijos asignados a un colaborador.
- Solo el personal autorizado por el Área de Tecnología esta facultado para abrir de manera física, un equipo de un colaborador o cualquier otro equipo de computo propiedad de QBCo S.A., Para los equipos de computo en esquema de arrendamiento directo, la empresa arrendadora es la única autorizada para abrir de manera física dichos equipos o en su caso autorizar la apertura de ellos.
- Todos los equipos de cómputo adquiridos directamente por QBCo o a través de las modalidades de Leasing, se encuentran bajo garantía, por lo que ningún colaborador debe tratar de realizar alguna reparación sobre el equipo ni contratar el mantenimiento del mismo.
- Todos los equipos de cómputo bajo la supervisión de QBCo. S.A. , deben contar con un Software antivirus actualizado y un firewall personal administrado por el personal del Área de Tecnología, con el objeto de proteger el equipo de software malicioso o peligroso para la información contenida en el misma.
- El usuario deberá reportar de forma inmediata al Área de Tecnología, cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas, golpes o peligro de incendio.

- El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.
- Es responsabilidad del usuario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.
- Cualquier persona que tenga acceso a las instalaciones de QBCo S.A., deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción o portería, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.
- Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos, sin la autorización del Área de Tecnología.
- Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos sobre los mismos.
- Se debe mantener el equipo informático en un lugar limpio y sin humedad.
- El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima, o en su defecto solicitar un reubicación de cables con el personal del Área de Tecnología.
- Cuando se requiera realizar cambios múltiples de los equipo de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con tres días de anticipación al Área de Tecnología a través de un plan detallado.
- Los usuarios deberán asegurarse de respaldar en copias de respaldo o backups, la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

- El usuario que tengan bajo su responsabilidad o asignados algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.
- El área de tecnología de QBCo S.A., establecerá en conjunto con los Gerentes de Cada Área, las correspondientes autorizaciones para el uso de dispositivos de almacenamiento externo, como Pen Drives o Memorias USB, Discos portátiles, Unidades de Cd y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups.
- El uso de los quemadores externos o grabadores de disco compacto es exclusivo para Backups o copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.
- Todo usuario deberá reportar al Área de Tecnología el uso de las memorias USB asignados para su trabajo y de carácter personal y responsabilizarse por el buen uso de ellas.
- Todo colaborador deberá informar en Portería, al momento de retirar de las instalaciones de la compañía, cualquier equipo de tecnología que pertenezca a QBCo S.A., además será responsable sobre toda la información e integridad del equipo y por ningún motivo podrá compartir información con terceros.
- Por ningún motivo el usuario podrá usar las impresoras para temas que no tenga que ver estrictamente con las labores que desempeña como colaborador en QBCo S.A.

## **CENTRO DE CÓMPUTO.**

En el centro de cómputo se alojan los servidores y equipos de comunicación necesarios para la operación de las actividades informáticas de la Empresa.

- El Acceso al centro de cómputo es restringido y solo personal autorizado por la Gerencia de Tecnología puede tener acceso a él.
- Solo el personal autorizado por el Área de Tecnología puede abrir los gabinetes de los servidores y de los demás equipos que se encuentran dentro del Centro de Cómputo.
- El Acceso a los servidores de QBCo S.A., ya sea usando la consola de administración local o una consola de administración remota es restringido a personal autorizado por la Gerencia de Tecnología. El intento de conexión por alguna persona no autorizada a cualquier consola de administración de los servidores se debe considerar una violación a las políticas de seguridad.
- El área de tecnología en cabeza de la Gerencia, establece las políticas y procedimientos administrativos para regular y controlar, el acceso de visitantes o funcionarios no autorizados a las instalaciones de cómputo restringidas.
- La Gerencia de Tecnología establecerá el responsable o administrador de cada uno de los centros de cómputo existentes en la organización.

## **PROPIEDAD DE LA INFORMACION:**

- Los usuarios de cualquier equipo de cómputo de QBCo S.A. deben ser conscientes que los datos que se crean y se trabajen en los sistemas, aplicaciones, desarrollos y cualquier medio de procesamiento electrónico, durante el desarrollo normal de sus actividades laborales, son propiedad y responsabilidad de QBCo S.A.
- Los derechos patrimoniales de un software, hojas de cálculo, archivos de procesamiento de palabra, archivos de presentaciones, bases de datos locales así como su documentación, creados por uno o varios colaboradores, en el ejercicio de sus actividades laborales, son de propiedad de QBCo S.A.
- Los respaldos de seguridad que contengan información que pertenece a QBCo S.A., y que fueron realizados a mutuo propio o por solicitud del usuario, se tendrán exclusivamente bajo resguardo, debiendo ser entregados en el momento de la finalización de la relación laboral.
- Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización respectiva, el usuario deberá notificar al Área de Tecnología la situación presentada.

## USOS INADECUADOS:

- Violar los derechos de cualquier persona o empresa protegidos por derecho de autor, patentes o cualquier otra forma de propiedad intelectual. Entre otras actividades se incluye la distribución o instalación de software sin licencia de uso adecuado adquirida por QBCO S.A.
- Difundir información identificada como confidencial a través de medios que involucren el uso de la tecnología de información.
- Introducir de manera dolosa, software malicioso o virus en el equipo, la red o servidores.
- Utilizar la infraestructura de tecnología de Información de QBCo S.A. para conseguir o tramitar material con ánimo de lucro. Igualmente se prohíbe el uso del sistema de información o de comunicaciones de QBCo S.A. con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil.
- Realizar actividades que coloquen en riesgo, la seguridad de los sistemas o aplicativos o que generen interrupción en la prestación de los servicios de tecnología.
- Monitorear puertos o realizar análisis de tráfico de la red con el propósito de evaluar vulnerabilidades de seguridad y dicho procedimiento no este autorizado por la Gerencia de Tecnología.
- Burlar mecanismos de seguridad físicos o lógicos, autenticaciones, autorizaciones de cualquier servicio de red, aplicación, servidor o cuenta de usuario.
- Instalar cualquier tipo de software en los equipos de cómputo de QBCo sin la previa autorización del Área de Tecnología.
- Modificar la configuración del software antivirus, firewall personales o políticas de seguridad en general implementadas en los equipos de cómputo de QBCo S.A., sin consultar previamente con el área de Tecnología, la cual analizara la viabilidad de los cambios solicitados.
- Reproducción de archivos de música o de video que no correspondan a temas estrictamente laborales, de capacitación, de conocimiento del área o de procesos de presentación formales de la empresa o actividades de mercadeo y comercial.

## **EXCEPCIONES.**

Para Propósitos de mantenimiento de la red y seguridad, algunos colaboradores de QBCo. S.A., pueden estar exentos de seguir algunas de las restricciones anteriores, debido a la responsabilidad de su cargo o a eventos programados.

Dichas excepciones se deberán establecer de manera clara, indicando la fecha de inicio y fecha final de la vigencia de la misma.

Toda excepción debe contemplar una caducidad en el tiempo de manera clara y concisa.

Estas excepciones deben ser solicitadas al Área de Tecnología, anexando la justificación respectiva vía correo electrónico o medio físico.

## POLITICA DE CONTRASEÑAS Y CLAVES.

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

### GENERALES.

- Todos los usuarios internos de QBCo S.A., requieren de un nombre de usuario y una contraseña para utilizar el equipo de computo que tiene asignado y servicios de red como correo electrónico, Intranet, Internet, Carpetas y Escritorios Compartidos.
- Las contraseñas son personales e intransferibles y deben ser conocidas únicamente por el propio usuario, el cual será responsable de toda actividad que se realice con ella.
- Por seguridad las contraseñas deben ser cambiadas de manera periódica máximo cada mes por el propio usuario.
- La Gerencia de Tecnología se reserva el derecho de restablecer en cualquier momento la contraseña de cualquiera de los usuarios de QBCo S.A., con previo aviso para no afectar de ninguna manera la continuidad de su trabajo, si se detecta que el mismo puede comprometer en algún proceso de riesgo a la organización.
- Todas las computadoras de escritorio y portátiles, deben tener configurado un protector de pantalla con clave y el cual se activara si el equipo se deja desatendido después de cierto tiempo.
- Las cuentas de correo electrónico y su contraseña, deberá ser solicitada para su creación, al Área de Tecnología, a través de un requerimiento formal de la Gerencia donde el colaborador prestara sus servicios.
- Toda persona que ingresa como usuario nuevo a QBCo S.A., para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información.
- Todo usuario que tenga la sospecha de que su contraseña, es conocida por otra persona, deberá cambiarla inmediatamente.
- Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione la facilidad de ser conocida o identificada.

## **USOS INADECUADOS:**

- Revelar su contraseña a personal no autorizado o permitir su uso a terceros para actividades ajenas a la misión de QBCo S.A., La prohibición incluye familiares y cualquier otra persona externa a la organización, cuando la conexión a la red de QBCo S.A. se realice físicamente fuera de la Empresa.
- Revelar su contraseña a otro colaborador de la Empresa.
- Anotar la contraseña de manera escrita y la misma se encuentre a la vista de todos en su lugar de trabajo.

## **POLITICA DE USO DE INTERNET Y CORREO ELECTRONICO.**

### **ADMINISTRACION.**

Los servicios de acceso a Internet y Correo Electrónico son administrados institucionalmente por el Área de Tecnología, quien tomara los reportes de los problemas técnicos y errores de recepción y envíos relacionados con nuestros servidores, para su posible atención inmediata. Sin embargo el proveedor del enlace de internet y del correo electrónico son los responsables por garantizar la disponibilidad del enlace y de los servicios contratados.

El Área de Tecnología esta facultada para monitorear periódicamente las actividades de cada uno de los usuarios de correo electrónico, Internet y comunicación por la red de datos de QBCo S.A., con la finalidad de vigilar el cumplimiento de las políticas del presente documento, manteniendo la confidencialidad de la información.

### **CORREO ELECTRONICO.**

- La comunicación institucional realizada por correo electrónico, solo será a través de las cuentas asignadas y aprobadas en su estructura.
- El correo electrónico es correspondencia privada entre el emisor y el destinatario, por lo tanto, no podrá transmitirse a través de Internet, información considerada como de uso confidencial hacia el personal externo de QBCo S.A., salvo instrucción expresa de la Gerencia a cargo del Área solicitante o del Área de Tecnología.
- El usuario es responsable del contenido de los mensajes enviados, esto incluye entre otros. Contenido de Material Ofensivo u Obsceno, cualquier uso de material con información ilegal o criminal.
- Se prohíbe la transmisión de mensajes que puedan crear un medio hostil sobre la raza, edad, condición sexual, religión, política, nacionalidad, origen, incapacidad u orientaciones personales, comentarios despectivos, noticias informales o mal intencionadas, cadenas de carta o de ayuda, mensajes masivos de índole personal, y en general cualquier tipo de información que cause congestión o alto trafico de la red o interfiera en el trabajo de otros.
- Los correos enviados a través de la cuenta de correo de la empresa debe ser utilizada para fines estrictamente enmarcados en la parte laboral de cada colaborador.
- El área de tecnología podrá bloquear la recepción y envío de correos electrónicos, desde una cuenta, donde se identifica el envío de correo basura, correo spam, virus o código malicioso en general. En caso de que el usuario necesite recibir correo electrónico desde alguna de estas direcciones identificada como ofensiva para QBCo S.A., debe comunicarse con el área de Tecnología para analizar y atender la solicitud.

- El área de tecnología informara el tipo de archivo que se podrá enviar o recibir como datos adjuntos en los correos electrónicos por parte de los colaboradores de QBCo S.A..
- Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de QBCo S.A.. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

## **INTERNET:**

- El usuario para poder tener acceso a Internet deberá solicitarlo al Área de Tecnología, previa autorización de la Gerencia a la cual el colaborador realiza sus actividades laborales.
- No acceder, ver o bajar desde sitios de internet: Gráficos, imágenes, documentos o cualquier otro material que se considera obsceno, vulgar, abusivo o que contenga información inapropiada, lenguaje amenazante, o que atente contra la dignidad de una persona.
- A cada usuario se le podrá asignar un perfil de navegación en dependencia con las actividades que realiza.
- El usuario no podrá vincular a la red inalámbrica de QBCo S.A con dispositivos móviles personales tales como Celulares, Smartphone, Tablets entre otros; y por ningún motivo podrán suministrar las claves de acceso a terceros o visitantes.
- Las Herramientas de Mensajería Interna deben ser utilizadas para fines estrictamente laborales y a las mismas solo deben agregarse como contactos, aquellos que correspondan a colaboradores de la Empresa QBCo S.A.

## **SEGURIDAD:**

- El área de tecnología es responsable de configurar a los usuarios el servicio correspondiente.
- Las cuentas y claves de acceso de los servicios de internet y correo electrónico son personales y confidenciales y se rigen por la política de contraseñas y claves definida en este documento.
- El usuario deberá notificar al Área de Tecnología cualquier uso no autorizado de su cuenta o cualquier violación a la seguridad de la misma.
- El usuario tiene la obligación de utilizar los servicios expresamente para fines institucionales de la Empresa QBCo S.A.
- Cualquier archivo o programa obtenido a través de Internet o Correo Electrónico debe ser revisado con software antivirus antes de ser almacenado en el equipo del colaborador.
- No debe utilizarse el correo electrónico en suscripciones a listas que saturen la capacidad de almacenamiento del buzón.
- Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el Área de Tecnología en aplicaciones como son Antivirus o Navegadores.

## **CLASIFICACION DE LA INFORMACION:**

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

- **CONFIDENCIALIDAD**

0- Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de QBo S.A. o no.

### **NIVEL PÚBLICO**

1- Información que puede ser conocida y utilizada por todos los empleados de QBCo S.A. y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para QBCo S.A., o a Terceros.

### **NIVEL RESERVADA – USO INTERNO**

2- Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a QBCo S.A., o a Terceros.

### **NIVEL RESERVADA – CONFIDENCIAL**

3- Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de QBCo S.A., y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves a QBCo S.A. o a Terceros.

### **NIVEL RESERVADA – SECRETA**

- **INTEGRIDAD:**

0- Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operación de QBCo S.A..

1- Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para QBCo S.A. o terceros.

2- Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para QBCo S.A. o terceros.

3- Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves para QBCo S.A. o a terceros.

- **DISPONIBILIDAD:**

0- Información cuya inaccesibilidad no afecta la operación de QBCo S.A.

1- Información cuya inaccesibilidad permanente durante Una Semana podría ocasionar pérdidas significativas para QBCo S.A. o terceros.

2- Información cuya inaccesibilidad permanente durante 2 a 5 Días podría ocasionar pérdidas significativas a QBCo S.A. o terceros.

3- Información cuya inaccesibilidad permanente durante 1 Día podría ocasionar pérdidas significativas a QBCo S.A. o terceros.

Al referirse a pérdidas, se contemplan aquellas cuantificables (materiales) y no cuantificables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

## **ALMACENAMIENTO,**

- La información obtenida de cualquiera de los servicios deberá ser almacenada localmente en el equipo de computo del usuario y no puede ser distribuida o transmitida por la red institucional, sin que el usuario garantice que la información contenida no presenta riesgos de virus, código malicioso o cualquier contenido que pueda afectar la seguridad de la información de la Organización.

## **PROPIEDAD Y DERECHOS DE CONTENIDO.**

- Los usuarios no deben descargar ni instalar cualquier tipo de software comercial, shareware o freeware en las unidades de disco, sin la autorización y conocimiento del Área de Tecnología.

## **CONDUCTA DEL USUARIO.**

- El usuario es el único responsable del contenido de las transmisiones a través de cualquier servicio.
- El usuario no debe usar el servicio para propósitos ilegales o de entretenimiento.
- El usuario debe cumplir con todas las regulaciones, políticas y procedimientos de Internet.
- La comunicación de los usuarios se debe conducir con respeto y consideración, evitando los abusos y el uso de lenguaje inapropiado.
- Se prohíbe el acceso a cualquier fuente de información cuyo contenido no se encuentre relacionado con las actividades de QBCo S.A. o con las actividades del colaborador.

## **POLITICA DE USO DE SOFTWARE.**

### **POLITICAS DE ADMINISTRACION:**

La Gerencia de Tecnología, es la única área autorizada para llevar a cabo la administración del software de QBCo S.A., por lo que dentro de sus responsabilidades tiene:

- Mantener bajo resguardo las licencias de uso de software.
- Llevar un control exacto de las licencias de operación y el equipo que se encuentra en uso.
- Establecer políticas y lineamientos para el uso de software, previa aprobación por parte de la Gerencia General y la Gerencia de Tecnología.
- Organizar la inspección de equipos de cómputo en intervalos regulares.
- Difundir la política de uso de software, con el fin que conozcan la normatividad en este rubro.
- Realizar un análisis de necesidades y requerimientos de software, con la finalidad de establecer prioridades de solución a las necesidades de información.
- Tendrá bajo su resguardo las licencias de software, CD de software y un juego de manuales originales, así como un CD de respaldo para su instalación, mismos que serán entregados por el área usuaria de la licencia, para llevar el control de software instalado, para los equipos informáticos de cómputo de escritorio, portátiles y periféricos al momento de la recepción de los mismos.

## **POLITICAS DE INSTALACION:**

- El área de Tecnología es la única área autorizada, así como responsable de realizar la instalación de software y proporcionar soporte del mismo, en todas las computadoras de la empresa. (propias y en modalidad de arrendamiento).
  
- Esta responsabilidad abarca:
  - Computadores de Escritorio
  - Computadores Portátiles

La Gerencia de Tecnología se compromete a instalar y proporcionar soporte sobre el software o, en su caso guiar el proceso de instalación, con el fin de operarlo de las mejores condiciones.

El usuario que ingrese equipos de su propiedad a las instalaciones de QBCo S.A., es responsable de la información almacenada en el mismo, y deberá mantener la privacidad, integridad y respaldos de la misma sin ser esto responsabilidad del Área de Tecnología.

En el caso de reinstalaciones de equipo, el usuario será el responsable de verificar que toda la información y archivos de trabajo estén contenidos en el equipo asignado,

El Área de Tecnología no es responsable de la configuración de dispositivos personales tales como Palms, Tablets, iPOD, teléfonos celulares o cualquier otro dispositivo propiedad del usuario.

El usuario que requiera la instalación de Software de su propiedad deberá solicitar por escrito al Área de Tecnología, anexando copia de la licencia que compruebe su propiedad o en el caso de software libre el documento probatorio.

Todo dispositivo de almacenamiento o instalación bajo el cual se entregue el software a las diferentes áreas de la organización, ya sea disco, memoria, disco externo. Una vez instalado en los equipos correspondientes, debe ser entregado, el original del mismo, al área de tecnología, el cual deberá etiquetarlo y guardarlo en un ambiente que permita la preservación de la información contenida en la misma.

## **SOFTWARE INSTITUCIONAL.**

La gerencia de tecnología de acuerdo con las disponibilidades existentes de software ha fijado un estándar para ser utilizado por las áreas usuarias. Todo equipo de cómputo antes de ser entregado al usuario final cuenta con dicho software, que es denominado Software Institucional.

Así mismo existe software adicional utilizado por el área de tecnología para efectos de soporte, desarrollo y monitoreo de información.

## **CONDICIONES BAJO LAS QUE PUEDE UTILIZARSE SOFTWARE ADICIONAL.**

- Software Preinstalado.
- Software proporcionado por el Área de Tecnología con el fin de:
  - Realizar actualizaciones remotas.
  - Actualizar Software Preinstalado.
  - Sustituir Software Preinstalado.
- Accesos o componentes de Software instalados en los servidores de información
- Software de uso emergente o temporal.

## **SOFTWARE DE SOPORTE O COMPLEMENTARIO.**

Identifíquese este software que es propiedad de alguna entidad gubernamental, bancaria y que requiere ser instalado para realizar, en tiempo y forma, las actividades encomendadas a los usuarios. Así mismo y dentro del mismo contexto se considera al software utilizado por el área jurídica, dado que se apoya en aplicaciones especializadas en el tema.

Por otro lado, también se encuentra el software que viene junto con algunos artículos (Cámaras, Grabadoras o Videograbadoras, Unidades de Respaldo, Unidades de Almacenamiento Externo, GPS o Periféricos) y que sin estas aplicaciones no pueden operar correctamente.

## **SOFTWARE QUE NO PUEDE SER INSTALADO:**

- Copias ilegales de cualquier Software.
- Software descargado de Internet sin autorización del Área de Tecnología.
- Software que no haya sido identificado como institucional.
- Instalaciones no autorizadas o que no hayan sido solicitadas al Área de Tecnología.
- Software adquirido para uso personal y sin fines institucionales.
- Software de esparcimiento o entretenimiento.
- Software de juegos.
- Software de desarrollo de aplicaciones no autorizado.

## **LICENCIAMIENTO.**

La mayoría del Software institucional se encuentra amparado por una licencia de uso (salvo las aplicaciones de uso libre con fines institucionales), las mismas que tienen un proceso de adquisición.

El objetivo del Área de Tecnología es mantener los controles de licenciamiento actualizado. Para cumplir con esta meta, se responsabiliza de mantener la disponibilidad de suficiencia de dichas licencias para el software clasificado como:

- Sistemas Operativos
- Aplicaciones
- Desarrollo
- Herramientas Especializadas
- Accesorios

Las clasificaciones adicionales de software, requieren para su instalación la adquisición adicional de licencias, debido a que se requiere para disponibilidades específicas, en caso de ser necesario, es el usuario quien tiene que justificar la adquisición, la cual deberá ser aprobada por la Gerencia a la cual el usuario se encuentre asociado.

Todo usuario que requiera un determinado software instalado en su computadora, deberá solicitarlo de acuerdo al formato establecido para tal fin.

El área de tecnología determinará, de acuerdo a las características del software que maneja, si existe disponibilidad de licencias para atender el requerimiento o, en su caso, si cuenta con el software solicitado, respondiendo oficialmente en cualquiera de ambos casos.

En caso de que la petición sea atendida satisfactoriamente, el Área de Tecnología actualizará y entregará la CARTA PERSONALIZADA DE USO DE SOFTWARE, al usuario responsable del equipo.

Si es necesaria la adquisición de nuevo software, el Área de Tecnología será la encargada de dicho trámite e informará al usuario solicitante sobre el avance del mismo.

## **USO DE SOFTWARE DESARROLLADO AL INTERIOR DE QBCo S.A.**

El uso de Software desarrollado al interior de QBCo S.A., no se encuentra sujeto a la limitación en cuanto al uso de licencias y las directrices en cuanto a su administración dependen de las áreas usuarias y responsables del mismo o, en su caso, de los controles o limitaciones tecnológicas de instalaciones requeridas en los equipos de los usuarios.

## **POLITICA INSTITUCIONAL.**

El uso de cualquier software sin licencia es ilegal y puede exponer a QBCo S.A., a una responsabilidad civil y penal bajo las leyes de derecho de autor, por lo que QBCo S.A. no tolerara la utilización de software sin licencia o no autorizado por el Área de Tecnología.

Así mismo, todo empleado que sea descubierto copiando software de manera ilegal o que copie software para entregárselo a un tercero, sin previa autorización, incluyendo clientes y proveedores, será sancionado de acuerdo a las circunstancias del caso.

El área de tecnología le corresponde la custodia de la información y velar por que la misma se encuentre bajo condiciones de seguridad y oportunidad para la organización. El área de tecnología no es dueña de la información existente en los diferentes módulos y aplicativos existentes en la empresa, por lo cual, ningún colaborador del área de TI esta autorizado para realizar labores de actualización, modificación, edición, eliminación a la información existente en las bases de datos de los aplicativos y software en general existente en la organización.

El área de tecnología podrá trabajar aquellos procesos referentes a cargue masivo de información a través de plantillas avaladas y certificadas por parte del proveedor y diligenciadas por las áreas correspondientes,

El área de tecnología no será responsable de la construcción o diligenciamiento de plantillas de cargue de información ni de los datos contenidos en las mismas.

## **POLITICA DE CAPACITACION.**

- La Asistencia y Puntualidad son requisitos indispensables a tomar en cuenta. Para este fin se establece que no se permitirá ninguna falta no justificada a cualquiera de las sesiones programadas dentro de un curso ofrecido por el Área de Tecnología.
- La Tolerancia para el ingreso será de 15 minutos máximo, pasado este tiempo, el colaborador no podrá ingresar a la sesión de capacitación.
- El uso de celulares no está permitido durante el desarrollo de las clases.
- El uso de portátiles, tablets, agendas electrónicas o cualquier otro dispositivo de comunicación, no está permitido durante el desarrollo de las clases. Los mismos deberán ser utilizados solo para los fines específicos objeto de la capacitación que se esté realizando.
- Asimismo, no se permitirá el ingreso de comida ó bebidas a las instalaciones donde se esté realizando la capacitación, a fin de mantener el los equipos en óptimas condiciones.
- Al final de cada curso se realiza una evaluación, siendo la nota mínima aprobatoria 75 puntos.
- Todos los cursos dictados están relacionados a las herramientas tecnológicas existentes en la Organización QBCo S.A. o en aquellas requeridas para las implementaciones de soluciones de software o hardware adquiridas o contratadas por la Empresa.
- Las actividades de capacitación que se realicen deberán estar acordes a la identificación de necesidades y requerimientos de las herramientas de tecnología existentes dentro de la Organización QBCo S.A., o a programas y herramientas tecnológicas nuevas que requieran de preparación especializada o puntual acerca de las mismas.

- Las fechas, horarios, ubicación y agenda se establecerán en común acuerdo con la persona encargada de la capacitación ya sea interna o externa y la misma deberá ser comunicada con una semana de anticipación a los participantes y a sus jefes respectivos, para de esta forma puedan programar sus actividades laborales y de logística.

## **COMPROMISO DE CONFIDENCIALIDAD**

Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de contrato, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de QBCo S.A.. La copia firmada del Compromiso deberá ser retenida en forma segura por el Área de Recursos Humanos o quien se designe para tal fin.

## RESGUARDO DE LA INFORMACION

El Área de Tecnología y los propietarios de información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

El Área de Tecnología dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico de la Empresa. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades de la Empresa.

Se definirán procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos:

- a) Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
- b) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.
- c) Almacenar en una ubicación remota, ya sea de manera física o virtual, copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos dos generaciones o ciclos de información de resguardo para la información y el software esenciales para la Empresa. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad (Clasificación de la información) y requisitos legales a los que se encuentre sujeta.
- d) Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.

e) Probar periódicamente los medios de resguardo.

f) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

## TERCERIZACION

Cuando exista la necesidad de otorgar acceso a terceras partes a información de QBCo S.A., el Área de Tecnología y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la seguridad de la información de la Empresa.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de QBCo S.A., se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

Se cita a modo de ejemplo:

- a) Personal de mantenimiento y soporte de hardware y software.
- b) Limpieza, guardias de seguridad y otros servicios de soporte tercerizados.
- c) Pasantías y otras designaciones de corto plazo.
- d) Consultores.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión, confidencialidad y acceso.

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y equipos de cómputo de QBCO S.A. contemplarán los siguientes aspectos:

- a) Cumplimiento de la Política de seguridad de la información.
- b) Protección de los activos de la Empresa, incluyendo:
  - Procedimientos para proteger los bienes de la Empresa, abarcando los activos físicos, la información y el software.
  - Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
  - Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
  - Restricciones a la copia y divulgación de información.
- c) Descripción de los servicios disponibles.
- d) Nivel de servicio esperado y niveles de servicio aceptables.
- e) Permiso para la transferencia de personal cuando sea necesario.
- f) Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
- g) Existencia de derechos de propiedad intelectual.
- h) Definiciones relacionadas con la protección de datos.
- i) Acuerdos de control de accesos que contemplen:
  - Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
  - Proceso de autorización de accesos y privilegios de usuarios.
  - Requerimiento para mantener actualizada una lista de las personas autorizadas a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

- j) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
- k) Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
- l) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
- m) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
- n) Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.
- o) Proceso claro y detallado de administración de cambios.
- p) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
- q) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
- r) Controles que garanticen la protección contra software malicioso.
- s) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.
- t) Relación entre proveedores y subcontratistas.

Adicionalmente se deberán tener en cuenta los siguientes aspectos:

- a) Forma en que se cumplirán los requisitos legales aplicables.
- b) Medios para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.
- c) Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos de la Empresa.
- d) Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible de la Empresa.
- e) Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
- f) Niveles de seguridad física que se asignarán al equipamiento tercerizado.
- g) Derecho a la auditoría por parte de la Empresa, sobre los aspectos tercerizados en forma directa o a través de la contratación de servicios ad hoc.

## **VIGENCIA DE LAS POLITICAS**

Estas políticas tendrán vigencia a partir de la aprobación de la Gerencia General y serán revisadas por la Gerencia de Tecnología, de acuerdo a los cambios en la Infraestructura, Aplicaciones o evolución tecnológica.

Las políticas tendrán una revisión periódica se recomienda que sea semestral para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones y sugerencias.

## SANCIONES

Al detectarse un Incumplimiento en las actuales políticas, se aplicaran los siguientes criterios y sanciones:

1. La primera vez que el usuario haya incumplido una de las políticas, la Gerencia de Tecnología notificara por escrito al responsable de la falta y le recordara las políticas vigentes.
2. De presentarse un segundo incumplimiento en las Políticas, la Gerencia de Tecnología notificara por escrito a la Gerencia del Área Correspondiente, informándole del tipo y contenido de la falta, suspendiendo el servicio temporalmente al usuario responsable hasta que el Gerente del Área apruebe por escrito la restauración del servicio.
3. En caso de presentarse un tercer incumplimiento en las políticas por parte del mismo usuario, causara suspensión inmediata y definitiva del servicio y el caso se enviara a la Gerencia de Recursos Humanos para determinar si es necesario aplicar sanciones administrativas o laborales. El área de tecnología se reserva el derecho de suspender el acceso a la red y al equipo de cómputo por parte del usuario de manera inmediata, si se considera que la seguridad de los datos y la información de la compañía se encuentra expuesta o comprometida.

## RECOMENDACIONES

Estas son algunas de las normas que le ayudaran a aprovechar al máximo el uso de los servicios de tecnología y comunicación existentes en QBCo S.A.:

- Ser respetuoso de sus compañeros de trabajo y de su trabajo
- Evitar dañar el computador.
- Respetar los derechos de autor.
- No compartir bajo ninguna circunstancia sus contraseñas y claves.
- No gastar recursos limitados tales como espacios en disco o capacidad de impresión.
- No acceder a los archivos de otras personas.
- Si se encuentra por accidente algún material ilegal u ofensivo, avisar inmediatamente al área de tecnología.
- Asumir la responsabilidad por sus propias acciones y por la perdida de servicios si existe alguna infracción a las políticas.
- Hacer uso adecuado de los servicios de tecnología y comunicaciones, piense que estos servicios son su herramienta de trabajo y no un pasatiempo. Cualquier aclaración o comentario, la puede hacer llegar al área de tecnología, extensiones 200 y 236.