



Políticas

*Para el uso y manejo de la
información y de los recursos
informáticos*



Las políticas para el uso de los recursos informáticos en Grupo Familia, dan a los usuarios las directrices y condiciones necesarias para alcanzar la confidencialidad, la integridad y la disponibilidad de la información. Este documento tiene como objetivo básico regular la forma cómo la Compañía maneja, protege y distribuye su información. Además, informa cómo se deben usar los recursos informáticos.

Es responsabilidad de todos, conocer y aplicar este conjunto de políticas. Por favor lea con detenimiento su contenido, al hacer uso de los recursos informáticos, el usuario acepta todos los términos y condiciones del mismo y se obliga a su entero cumplimiento. Grupo Familia se reserva el derecho de modificar cualesquiera de las políticas aquí contenidas, en cualquier momento y a su sola discreción, por el solo hecho de publicar una nueva versión de los mismos.

El contenido del presente documento está protegido por las normas de la Propiedad Intelectual, cuyos derechos recaen exclusivamente en Grupo Familia.

Juan Esteban Jaramillo Jiménez
Gerente División Tecnología de Información



Políticas *relacionadas con la Propiedad y Uso de la Información*

Propiedad de la información

Toda la información almacenada en los sistemas de información y dispositivos suministros por la Compañía, que contengan información generada o relacionada con la misma o desarrollada por los empleados o proveedores es propiedad exclusiva de Grupo Familia, protegida por las normas que regulan la Propiedad Intelectual. En consecuencia, la información no podrá ser divulgada, usada, distribuida, publicada, reproducida, transmitida o fijada en cualquier soporte material conocido o por conocerse y en general realizarse cualquier acto de disposición sobre la información salvo que exista una autorización expresa y en contrario por parte de la Compañía.

Así mismo toda la información almacenada en los sistemas de información y dispositivos suministrados por la compañía, será susceptible de ser revisada, en caso de ser requerido, por la Gerencia de Tecnología de Información, previa solicitud y autorización de la Gerencia de Desarrollo Organizacional. La compañía revisará la información bajo los parámetros de la diligencia debida respecto de la información personal de los usuarios, en aras de salvaguardar el derecho a la intimidad y no divulgación y conservará la información personal bajo las condiciones de seguridad que considere necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Cuando los datos personales no tengan el carácter de públicos, la Compañía garantiza la reserva de la información en todo tiempo con carácter confidencial.



Uso de la información

Solo el usuario es responsable de darle un debido uso a la información a la cual tiene acceso y tratarla con suma diligencia y cuidado.

La Compañía cuenta con los mecanismos para salvaguardar la información del negocio, pero es responsabilidad del usuario, realizar el proceso de copia de respaldo de la información de su estación de trabajo, en la ubicación que se ha asignado para ello.

Los sistemas de información permiten compartir información para facilitar las actividades de colaboración, el buen uso de ésta es fundamental para no poner en riesgo el negocio.

Al compartir información, asegúrese que la misma no tenga carácter confidencial, que no se trate de información protegida como secreto empresarial o industrial, en cuyo caso la misma no podrá ser revelada bajo ninguna circunstancia salvo que la Compañía autorice su revelación previa firma de los respectivos acuerdos de confidencialidad. Al compartir información asegúrese que está brindando acceso a ésta, a las personas que efectivamente lo requieren. Esta característica de colaboración se debe utilizar para actividades propias del negocio, no se debe compartir información de carácter personal.

No se debe utilizar los sistemas de información ni dispositivos de la Compañía, para transmitir o distribuir material comercial, difamatorio, obsceno, abusivo, ilegal, peligroso, ofensivo, que invadan la privacidad o violatorio de derechos de autor, marcas o patentes pertenecientes a la Compañía o de terceros.

Se prohíbe violar la seguridad de cualquier contenido, incluyendo el acceder a la información sin estar autorizado.

La información privada suministrada a la compañía, por los usuarios, se reserva sólo para la Compañía y no será divulgada a otros medios.



Políticas para las Cuentas de Usuario en Red

Una cuenta de usuario es un identificador que se le asigna a una persona en un sistema. A partir del momento de la asignación, el usuario será responsable del uso adecuado de los diferentes servicios que dicha cuenta posee (utilización de recursos como impresión, correo electrónico, modificación de información, entre otros).

Para esto se debe tener en cuenta lo siguiente:

Caducidad

Es el tiempo máximo durante el cual un usuario de red puede ingresar al sistema con la misma contraseña. Una vez transcurrido este tiempo, el sistema lo obligará a cambiarla.

- La caducidad de la contraseña es de 30 días.
- Para el cambio obligado de la contraseña el sistema le avisará con anterioridad.

Naturaleza

Los usuarios deben seguir las normas de seguridad mínima a la hora de escoger adecuadamente la contraseña para el acceso. Por esta razón, cuando se asigna una nueva contraseña, tenga en cuenta las siguientes restricciones:

- No se puede utilizar el mismo nombre que tiene como usuario.
- No se puede utilizar los nombres o apellidos relacionados con el usuario.
- La longitud de la contraseña, debe ser mínimo 8 caracteres y máximo de 40. Estos deben ser letras, números y/o símbolos.
- Si va a utilizar sólo números y letras, tenga en cuenta que al menos una de ellas debe ser mayúscula.

Ejemplos válidos:

Inicio2012 ó inicio.2012

- La contraseña debe ser diferente a las últimas 13 utilizadas.



Inactivación: cuando se deshabilita una cuenta de usuario de Red

La cuenta del usuario será deshabilitada si:

- Han pasado 30 días sin que el usuario haya iniciado sesión en la red.

En este caso, si se requiere habilitar nuevamente la cuenta, se debe seguir los lineamientos dados en el documento **Acuerdo de Nivel de Servicio**, en la parte donde se mencionan las autorizaciones.

- El usuario termina su relación laboral con la Compañía, y Desarrollo Organizacional notifica del evento al personal Centro de Atención al Usuario.

En este caso sólo se habilitará nuevamente la cuenta de usuario, tras la solicitud de Desarrollo Organizacional.

Responsabilidades de los empleados frente al uso de su cuenta de usuario de red

- El titular de la cuenta de usuario es el único responsable de todas las operaciones que se realicen con ésta.
- La cuenta de usuario es personal e intransferible.
- Cuando ante una revisión técnica si debe proporcionar su clave de red al personal del Centro de Atención al Usuario, ésta será reestablecida por una estándar cuando finalice el procedimiento. Cuando usted ingrese nuevamente el sistema le pedirá que cambie dicha clave por una que solo usted conozca.



Acceso a la Red Corporativa

- Los privilegios asignados a un usuario para conectarse remotamente a los sistemas de información son para uso exclusivo del usuario titular. Por esta razón no está permitido facilitar dichos accesos a otros usuarios no autorizados.
- Los equipos personales o de proveedores externos no pueden ser conectados a la red corporativa sin previa autorización de la Gerencia de Tecnología de Información. Utilizar equipos diferentes a los autorizados pone en riesgo la seguridad de la información.
- Los puntos de acceso inalámbricos que posee la compañía tienen una configuración especial con el fin de restringir el acceso de personas ajena a la compañía.
- En algunas sedes de la compañía se cuenta con una red para invitados, la cual sólo puede ser utilizada por proveedores y accionistas. La excepciones requieren autorización de la Gerencia de Tecnología de Información.



Políticas aplicadas a las Estaciones de Trabajo

- Las estaciones de trabajo se bloquean automáticamente a los 30 minutos de no detectar actividad.

Para desbloquear el equipo es necesario digitar de nuevo la contraseña de red.

- Después de 2 horas de no detectar actividad, las estaciones de trabajo quedan en modo ahorro de energía (hibernación).

- Todos los usuarios de estaciones de trabajo poseen privilegios limitados para realizar configuraciones en éstas (Rol usuario).

- Se podrá establecer un papel tapiz y un protector de pantalla a nivel corporativo para las estaciones de trabajo: estos cambiarán de acuerdo a los lineamientos dados por la Gerencia de Desarrollo Organacional.

- No está permitido crear en las estaciones de trabajo usuarios locales.

- Después de la realización de tareas de mantenimiento programado de carácter obligatorio, el desempeño de su estación de trabajo, se podrá ver disminuido temporalmente.

- Los dispositivos de entrada y salida serán monitoreados y según se considere necesario por la Gerencia de Tecnología de Información, su uso será restringido.

- Si las herramientas de seguridad informáticas no están funcionando adecuadamente en su estación de trabajo, su acceso a la red será limitado (Lync y correo electrónico).

- Las herramientas de seguridad informática instaladas en su estación de trabajo, podrían eliminar información de manera automática si ésta se encuentra afectada por alguna amenaza informática (virus).

- Las actividades realizadas en las estaciones de trabajo están sujetas al monitoreo de la Gerencia de Tecnología de Información a través del personal del Centro de Atención al Usuario.

- Para la adquisición de estaciones de trabajo se siguen ciertas líneas de configuración ya determinadas por la Gerencia de Tecnología de Información.

Éstas son:

- Línea de configuración de usuario estándar.
- Línea de configuración de usuario estándar móvil.
- Línea de configuración de usuario avanzado.
- Línea de configuración para Gerentes.

Estas líneas de configuración para estaciones de trabajo, están en el documento Arquitectura de Tecnología.

-Es responsabilidad de los usuarios que tienen habilitado el servicio de Unidad Segura, garantizar que su información crítica y sensible esté alojada en dicha unidad.



Políticas *relacionadas con los Servidores de Archivos*

Un servidor de archivos es un equipo de cómputo destinado a guardar la información que poseen los usuarios en sus estaciones de trabajo.

Acceso a la Carpeta de Respaldo

- Los usuarios son los únicos responsables de realizar el proceso de copia de la información que considere más importante, desde su estación de trabajo hacia su carpeta de respaldo, en el servidor de archivos. El Centro de Atención al Usuario estará disponible para indicarle el procedimiento para acceder a su carpeta de respaldo.
- En el caso de ocurrir algún incidente con el dispositivo de almacenamiento de las estaciones de trabajo, solo se logrará recuperar la información almacenada en la carpeta de respaldo.
- Solo cada usuario, posee acceso a su carpeta de respaldo.
- La carpeta de respaldo estará identificada en la estación de trabajo, como la unidad Z.

Tamaño de la Carpeta de Respaldo

- Cada usuario tiene en su carpeta de respaldo una capacidad de almacenamiento limitada. Para conocer el tamaño asignado para esta carpeta, consultar el documento Arquitectura de Tecnología.
- La capacidad de almacenamiento de su carpeta de respaldo puede ser modificada, solicitándolo a través del Centro de Atención al Usuario.



Contenido de la Carpeta de Respaldo

- En las carpetas de respaldo sólo debe estar almacenada información relacionada con el negocio.
- No está permitido instalar ningún tipo de aplicación en las carpetas de respaldo.

Carpetas Compartidas

- Estas carpetas son creadas para que la información usada por personas que tienen labores compartidas encuentren dicha información en un sitio común. Según la necesidad de almacenamiento de información se asigna la capacidad de estas carpetas.
- Cada carpeta compartida tiene un administrador quien es el responsable de otorgar los accesos requeridos y velar por su contenido.
- Para crear una carpeta compartida se debe seguir los lineamientos dados en el documento **Acuerdo de Nivel de Servicio**.



Políticas de Copia o Back Up de la Información

- A la información contenida en los servidores de archivos se le realiza copia de seguridad todos los días y se mantiene por un espacio de 15 días.
- La copia de información de los usuarios que tienen el servicio de back Up automático, se realiza inmediatamente hay una modificación y se mantiene por un espacio de 15 días.



Políticas del servicio de Correo Electrónico

Una cuenta de usuario puede tener asociado un buzón de correo electrónico si es requerido, donde toda la información transmitida por este medio es considerada como propiedad de la Compañía. Tenga en cuenta los siguientes aspectos para su adecuada utilización:

- No se puede transmitir información cuyo contenido sea ilegal, peligroso, pornográfico, ofensivo a terceros o que invadan la privacidad o violatorio de derechos de autor, marcas o patentes de la compañía o de terceros. No se puede transmitir información con carácter confidencial, protegida como secreto empresarial o industrial, salvo que la compañía autorice su revelación previa firma de los respectivos acuerdos de confidencialidad.
- No se puede transmitir información personal de propiedad de empleados, dependientes, contratistas o subcontratistas de la compañía y de terceros ajenos a la misma, salvo cuando existan las respectivas autorizaciones del titular de dicha información.
- No se puede suplantar a otra persona, para hacer declaraciones falsas o falsificar la identidad de alguna persona, en los encabezados de los mensajes transmitidos.
- No está permitido enviar mensajes no solicitados o autorizados por los destinatarios; promociones, cadenas, solicitudes o con archivos adjuntos que contengan virus, programas o códigos con capacidad para dañar equipos de cómputo de terceros.

Tamaño de los Buzones y Mensajes

- Los buzones de correo electrónico tienen un tamaño de almacenamiento limitado. Igualmente el tamaño máximo de los mensajes a recibir o enviar está predeterminado.
- Los tamaños asignados tanto para buzones, como para mensajes de correo electrónico, se encuentran definidos en el documento Arquitectura de Tecnología.



Tipos de Archivos No permitidos

- Por seguridad y rendimiento del servicio de correo electrónico no está permitido enviar ni recibir a través del correo cierto tipo de archivos.

Las extensiones que se encuentran excluidas están detalladas en el documento Arquitectura de Tecnología.

- La compañía cuenta con software que filtra el correo electrónico, liberando al usuario de mensajes tipo SPAM.

- El sistema antivirus y el software de filtrado que posee la compañía, además de eliminar automáticamente los archivos adjuntos con extensiones no permitidas, elimina los correos electrónicos que contengan cualquier manifestación de virus o software espía. Dada la frecuencia con la que esto ocurre, se ha deshabilitado a los usuarios finales la opción de notificarles cuando esta acción suceda.

Listas de distribución

Es una lista de direcciones de correo electrónico que se usa para enviar mensajes a un grupo de personas que comparten un rol, actividad o proyecto.

Algunas listas de distribución están restringidas, pues solo algunos usuarios pueden enviar mensajes a éstas. Mayor información en el documento Arquitectura de Tecnología.



Carpetas Personales

Las carpetas personales es un archivo que permite tener almacenado en las estaciones de trabajo correos electrónicos.

Por lo general esta carpeta personal se almacena en la unidad de almacenamiento principal del equipo del usuario (Disco Duro). En caso tal que dicha unidad de almacenamiento falle, la información contenida allí junto con la carpeta personal se perderá.

La ubicación de la carpeta personal puede ser configurada por el usuario teniendo en cuenta lo siguiente:

- Cada usuario es responsable de la ubicación física que le dará al archivo de carpetas personales.

- Es responsabilidad de cada usuario, realizar una copia en la carpeta de respaldo, con el fin de mantener copia de la información más importante.

Uso del Correo Electrónico por Internet

Permite acceder al servicio de correo electrónico desde cualquier parte del mundo usando un computador con conexión a Internet.

- Cualquier usuario puede hacer uso del OWA (Outlook Web Access) para acceder al correo desde la red corporativa o fuera de ella.



Retención de Elementos Eliminados del Buzón del Correo Electrónico

- Si un mensaje de correo electrónico es eliminado definitivamente, es decir, eliminado de la carpeta de "elementos eliminados", éste podrá ser recuperado si no han pasado más de 2 días desde el evento de borrado. Las únicas excepciones son aquellos mensajes que fueron borrados por el usuario usando la combinación de teclas SHIFT-DELETE (SHIFT-SUPRIMIR).

Carpetas Públicas del Correo Electrónico

Una carpeta pública es un espacio en el servidor de correo que permite recolectar, organizar y compartir información con otros usuarios que posean correo electrónico. Estas carpetas se pueden visualizar por medio del programa Outlook.

- Cada carpeta pública tiene un usuario o grupo de usuarios que administran la carpeta. El administrador(es) es responsable de otorgar los accesos requeridos y velar por su contenido.
- El tamaño máximo del mensaje o archivos contenidos en una carpeta pública es limitado. Las definiciones sobre este aspecto están en el documento Arquitectura de Tecnología.
- Para crear nuevas carpetas o subcarpetas se requiere hacer la solicitud al Centro de Atención al Usuario y seguir los lineamientos del documento Acuerdo de Nivel de Servicio.
- Si un archivo almacenado en una carpeta pública es eliminado, este se puede recuperar si no han pasado más de 2 días desde este suceso. Las únicas excepciones son aquellos mensajes que fueron borrados por el usuario usando la combinación de teclas SHIFT-DELETE (SHIFT-SUPRIMIR).



Políticas del Servicio de Navegación en Internet

La compañía cuenta con el servicio de Internet para sus usuarios como herramienta de trabajo.

- Los usuarios pueden utilizar el servicio de Internet para acceder a páginas de proveedores, entidades financieras, investigación, competencia, universidades, medios de comunicación, clientes y en general páginas que permitan mejorar o agilizar actividades del negocio.
- Se tiene restringido la navegación hacia las páginas que la compañía considera innecesarias para el desarrollo normal de las funciones. Esto aplica para los servicios de Internet dentro de la red corporativa y fuera de ella.
- Está restringida la descarga de cierto tipo de archivos como música, videos, programas y archivos de gran formato principalmente.
- La compañía utiliza un software de filtrado de contenido que registra las páginas que visitan los usuarios. A los usuarios que navegan en páginas no relacionadas con actividades del negocio, se le restringirá el acceso al servicio de navegación.
- No está permitido el uso, al interior de la compañía, de otro tipo de conexión a Internet diferente al establecido por la Gerencia de Tecnología de Información del Grupo Familia.



Políticas para las Cuentas de Usuario SAP

Con el fin de asegurar la confidencialidad de la información se han implementado las siguientes políticas de seguridad en el sistema SAP.

- La caducidad de la contraseña es de 30 días.
- La longitud de la contraseña debe ser mínimo de 8 caracteres y máximo de 40.
- La contraseña para ingresar al sistema SAP distingue entre mayúsculas y minúsculas.
- La contraseña debe estar conformada mínimo por 4 letras y mínimo 2 números.
- La contraseña debe ser diferente a las últimas 13 utilizadas.
- Para restablecer la contraseña acceda al servicio de cambio de contraseñas que se encuentra en Conéctate.
- Cuando al ingresar al sistema SAP el usuario digita mal 6 veces la contraseña, inmediatamente se bloquea el usuario.
- Las cuentas de usuario SAP no se crean genéricas, las excepciones serán evaluadas por el equipo de Tecnología de Información.
- Las cuentas de usuario SAP no se crean desde copias de otra cuenta de usuario la única excepción es el caso de practicantes o aprendices.



Inactivación: cuando se deshabilita una cuenta de usuario de SAP

La cuenta del usuario SAP será deshabilitada si:

- Han pasado 30 días sin que el usuario haya iniciado sesión en el sistema SAP. En este caso, si se requiere habilitar nuevamente la cuenta, el usuario debe hacer la solicitud por medio de su buzón de correo de la compañía al personal de Centro de Atención al Usuario.
- El usuario termina su relación laboral con la compañía y Desarrollo Organizacional notifica del evento al personal del Centro de Atención al Usuario. En este caso se deshabilita la cuenta de usuario SAP y se retiran todos los permisos. Ante este evento, sólo se habilitará nuevamente la cuenta de usuario SAP tras la solicitud de Desarrollo Organizacional.
- Desarrollo Organizacional es responsable de notificar al personal del Centro de Atención al Usuario, cualquier ausencia de un empleado que supere a los 5 días hábiles y la duración de dicha ausencia, con el objetivo de limitar el acceso a SAP por parte del usuario durante el período de tiempo notificado.

Autenticación de un Usuario de SAP

- Solo se podrá realizar la autenticación de un usuario de SAP desde una sola estación de trabajo.
- Luego de haber ingresado a SAP un usuario solo puede abrir máximo 4 modos.
- La conexión con SAP se cerrará automáticamente después de una hora de la última acción del usuario en el sistema.



Responsabilidades de los empleados frente al uso de su cuenta de usuario de SAP

- El titular de la cuenta de usuario es el único responsable de todas las operaciones que se realicen con ésta.
- La cuenta de usuario es personal e intransferible.



Políticas sobre el uso de los dispositivos de la Plataforma Tecnológica

Estas políticas rigen el uso de todos dispositivos informáticos que la compañía proporciona a los usuarios para realizar sus funciones.

- Los dispositivos asignados a los usuarios por la compañía, deben ser utilizados para fines relacionados con el negocio y no para fines personales.
- El usuario debe revisar y firmar el documento que acompaña la entrega de cualquier dispositivo otorgado por la compañía. Con esto, se compromete a cumplir los puntos que allí se especifican y los lineamientos consignados en este documento.
- No se debe alterar la configuración con la que le fue entregado su dispositivo. En estos, no se debe instalar nuevo software o hardware, tampoco es permitido desinstalar o inhabilitar el software que ya tiene instalado.
- En caso de una eventual falla en el dispositivo de almacenamiento, sólo se intentará recuperar la información relacionada con el negocio.
- La Gerencia de Tecnología de Información a través del Centro de Atención al Usuario, podrá eventualmente acceder a los dispositivos asignados a un usuario para verificar que no exista información no relacionada con el negocio.
- Las únicas personas que pueden interactuar a nivel técnico con los dispositivos asignados por la Compañía son aquellos que pertenecen al Centro de Atención al Usuario.
- Es responsabilidad de los usuarios que tienen a su cargo dispositivos asignados por la compañía, velar por el buen estado de los mismos.
- Toda contratación de servicios tecnológicos, software o dispositivos, deben estar avalados por la Gerencia de Tecnología de Información, previo a la ejecución de la compra.
- Las únicas personas que pueden hacer uso de los dispositivos, son aquellas vinculadas a la compañía, salvo algunas excepciones en las cuales los dispositivos de la compañía son manipulados por proveedores o personal temporal, casos en los cuales el personal del Centro de Atención al Usuario debe estar notificado.
- Los usuarios sólo podrán hacer uso de las impresoras departamentales, a las cuales tenga autorización.



- Está prohibido conectar a la red corporativa los siguientes dispositivos, por parte de los usuarios:
 - Enrutadores
 - Puntos de acceso inalámbrico
 - Concentradores (switch)
 - Analizadores de tráfico
- No está permitido imprimir documentos que no tengan relación con el negocio. El servicio de impresión es monitoreado por el personal de Centro de Atención al Usuario y es de carácter limitado por usuario mensualmente.
- Ante cualquier falla en los dispositivos entregados por la compañía, evite manipularlo sin el acompañamiento del personal del Centro de Atención al Usuario.
- El servicio de impresión se tiene centralizado en impresoras láser que soporan altas cargas de impresión. Por esta razón no se adquieren impresoras locales (conectadas directamente al equipo del usuario). Toda excepción, deberá ser analizada y autorizada por la Gerencia de Tecnología de Información.
- El software con licenciamiento limitado instalado en los dispositivos de los usuarios, podrá ser removido por el personal de centro de Atención al Usuario, si este no ha sido utilizado durante los últimos tres meses.
- Es responsabilidad de la Gerencia de Tecnología de Información, garantizar que todo software instalado en los dispositivos de la Compañía, sea licenciado, que sea estándar del mercado y que se aplique a los usuarios acorde a las necesidades y funciones de su cargo.



Políticas para el uso de Dispositivos Móviles

Cuando el dispositivo móvil es otorgado al usuario por la compañía, tenga en cuenta:

- El usuario es el responsable del buen uso y estado del dispositivo entregado por la compañía.
- Se configura en el dispositivo, un mecanismo de seguridad o contraseña que busca proteger la información almacenada en éste.
- Ante cualquier falla en los dispositivos móviles entregados por la compañía, evite manipularlo sin el acompañamiento del personal del Centro de Atención al Usuario.
- El uso de los dispositivos móviles otorgados por la compañía es principalmente para habilitar la realización de las actividades y funciones laborales del empleado.

Cuando los dispositivos móviles no son otorgados por la compañía, tenga en cuenta los siguientes puntos:

- La Gerencia de Tecnología de Información suministrará a los usuarios, diferentes servicios tecnológicos que podrán ser utilizados desde estos dispositivos siempre y cuando el usuario, cuente con las autorizaciones requeridas.
- Se entregará al usuario los parámetros o instructivos que el personal de centro de Atención al Usuario tenga disponibles, para que el usuario configure su dispositivo y pueda acceder a los servicios tecnológicos disponibles en la compañía.

En estos casos no se presta soporte ni asistencia técnica por parte del personal del Centro de Atención al Usuario.



Políticas

***para el uso de
equipos relacionados con el
Sistema de Comunicaciones
Unificadas***

- Es responsabilidad de la Gerencia de Tecnología de Información, suministrar a los usuarios los recursos necesarios para el uso del servicio de Comunicaciones Unificadas.
- El servicio de Comunicaciones Unificadas incluye: videoconferencia, comunicación de voz, mensajería instantánea, uso de aplicaciones compartidas, conferencias web o reuniones en línea, buzón de voz, mensajería unificada.
- Para el servicio de envío y recepción de fax se debe utilizar el sistema que la Gerencia de Tecnología de Información ha implementado.
- El uso de herramientas de mensajería instantánea externa, se hará exclusivamente a través de la plataforma de Comunicaciones Unificadas.
- La plataforma autorizada para realizar asistencia remota, es la que se encuentra incluida dentro de los servicios de Comunicación Unificada.



Políticas sobre el Desarrollo de Software

- Todo software desarrollado por o para la compañía, será de su entera propiedad.
- Solo la Gerencia de Tecnología de Información, está autorizada para desarrollar nuevas soluciones de software o contratarlas con un tercero.
- Si un área de la compañía desea automatizar algún proceso o mejorar uno existente, deberá solicitar formalmente este requerimiento a la Gerencia de Tecnología de Información, enviando un mensaje de correo electrónico al buzón del Centro de Atención al usuario.
- En caso tal que se realice un desarrollo, sin contar con la aprobación de la Gerencia de Tecnología de Información, éste no tendrá soporte técnico por parte del personal del centro de Atención al Usuario.



Políticas

sobre la prestación del servicio de Soporte Técnico a la Plataforma Tecnológica

- La Gerencia de Tecnología de Información ha estructurado la prestación del servicio de soporte técnico para la plataforma tecnológica que administra, a través de un único punto de contacto llamado Centro de Atención al Usuario. Los parámetros con los cuales este ente opera se encuentran detallados en el Acuerdo de Nivel de Servicio.



Sugerencias generales

-El buen manejo de la información, como uno de los activos más importantes de la compañía, es compromiso y responsabilidad de todos.

Tenga siempre presente las siguientes sugerencias:

Para las Cuentas de usuario

- No es recomendable el cambio de las contraseñas, los días viernes o días que anteceden a descansos largos como vacaciones o puentes festivos, ya que a su regreso puede olvidarla.
- Se recomienda cambiar la contraseña días antes de vencerse.
- No ponga por escrito su contraseña. No la deje expuesta.
- No digite su contraseña mientras alguien esté observando su teclado.
- Por seguridad es recomendable que acostumbre bloquear su equipo cada vez que tenga que ausentarse de su puesto de trabajo.

Para la información almacenada en los Servidores de Archivos

- Guarde periódicamente, la información más relevante relacionada con el trabajo en su carpeta de respaldo en el servidor de archivos. Si no posee dicha carpeta o no sabe como usarla consulte con el Centro de Atención al Usuario.
- Mantenga depurada su información, es decir, elimine la información redundante o desactualizada esto ayuda a mejorar el desempeño de sus dispositivos.
- Guarde todos sus datos en una única ubicación en su estación de trabajo, para facilitar su búsqueda, depuración y copias de respaldo.



Para el servicio de Correo Electrónico

- Solo envíe el mensaje de correo a las personas implicadas en el tema, esta recomendación se hace más importante si esta enviando archivos adjuntos.
- Es recomendable que las carpetas personales no tengan un tamaño superior a 2 GB.
- No abrir correos electrónicos de remitentes desconocidos. Elimínelos inmediatamente.
- Si desea modificar un archivo adjunto, primero guárdelo en su estación de trabajo antes de ejecutarlo.
- Evite enviar cadenas de correos electrónicos a personas de la compañía o terceros.

Para el uso de los dispositivos de la Plataforma Tecnológica

- Cuide sus dispositivos, no ingiera alimentos cerca de ellos. Recuerde que estos están bajo su responsabilidad.
- Si usted detecta que un dispositivo de la plataforma tecnológica presenta problemas, reporte esta situación al centro de Atención al Usuario, no intente repararlo usted mismo.
- Si utiliza equipo portátil y tiene que transportarlo, llévelo en un maletín adecuado y antes de trasladarlo verifique que se encuentre apagado.



Relación de las políticas para el uso de los recursos informáticos con el reglamento interno de trabajo

Estas políticas para el uso de los recursos informáticos son esenciales para el buen funcionamiento de los recursos que administra la Gerencia de Tecnología de Información. El cumplimiento de estas políticas salvaguarda uno de los activos más importantes que posee la compañía: la información. Por lo tanto, cualquier acción por parte del empleado que conlleve a infringir estas políticas podría ser causal de una sanción disciplinaria a nivel laboral. Lo anterior aplicando el reglamento interno de trabajo:

Capítulo XVI *Obligaciones especiales para la empresa y los Trabajadores*

Artículo 56:

Son obligaciones especiales del trabajador:

2. No comunicar a terceros, salvo autorización expresa, las informaciones que tenga sobre su trabajo, especialmente sobre las cosas que sean de naturaleza reservada o cuya divulgación pueda ocasionar perjuicios al empleador, por ejemplo: información sobre procesos, materias primas utilizadas, despachos, clientes, y en general, dar información sobre cualquier aspecto de la compañía que, como se indicó antes pueda afectarla, lo que no obsta para denunciar los delitos o violaciones del contrato o de las normas legales del trabajo, ante las autoridades competentes.

14. Manipular cuidadosamente y de acuerdo con las instrucciones recibidas, las máquinas, herramientas, productos, elementos de trabajo, etc., para evitar su pérdida, deterioro, accidentes de trabajo, enfermedades profesionales o cualquier otro riesgo.

16. Dar un uso adecuado al Internet y a las licencias de software, y emplearlos exclusivamente para los fines relacionados con el trabajo asignado.



Capítulo XVII Prohibiciones especiales para la empresa y los Trabajadores

Artículo 58:

Se prohíbe a los trabajadores:

1. Sustraer de la fábrica, taller o establecimiento útiles de trabajo, materias primas, productos elaborados, o cualquier elemento de la compañía sin el permiso correspondiente, así como consumirlas dentro de la empresa.
40. Tomar alimentos en el sitio de trabajo.
43. Dar un uso indebido al Internet o a las licencias de software, o utilizarlos para fines diferentes al trabajo asignado.

Capítulo IXX

**Despidos con o sin justa causa
Terminación de los contratos de trabajo**

Artículo 66

Son justas causas para dar por terminado unilateralemente el contrato de trabajo:

1. Por parte de la compañía:
 - 1.4. Todo daño material causado intencionalmente a los edificios, obras, maquinarias y materias primas, instrumentos y demás objetos relacionados con el trabajo y toda grave negligencia que ponga en peligro la seguridad de las personas o de las cosas.
 - 1.8. El que el trabajador revele los secretos técnicos o comerciales o dé a conocer asuntos de carácter reservado, con perjuicio para la compañía.

Para los efectos del Artículo 7 del Decreto 2351 de 1965, se califican como graves las siguientes faltas, además de las que tengan ese carácter en forma general:

7. La revelación de cualquier secreto o acto reservado relacionado con los negocios del empleador, aún por la primera vez.



12. Dañar las edificaciones, materiales, equipos, herramientas y otros elementos, pertenecientes a la compañía, intencionalmente o por descuido, aún por la primera vez.
25. Distribuir material escrito o impreso de cualquier clase dentro de las dependencias de la compañía, sin autorización, aún por primera vez.
28. Exhibir o entregar documentos o facturas, libros, herramientas, equipos, etc., de la compañía sin autorización, aún por la primera vez.
30. Dejar herramientas, elementos o equipos en sitios distintos a los señalados para tal fin o entregarlos sin recibir las órdenes correspondientes, aún por la primera vez.
40. Dar uso indebido al Internet o a las licencias de software, o utilizarlos para fines diferentes al trabajo asignado, aún por la primera vez.



Validez de las políticas para el uso y manejo de la información y los recursos informáticos

Si se llegara a determinar que algún término, condición o disposición de estas políticas es ilegal, inválida, nula o, por cualquier razón, inaceptable, la validez y aplicación de las demás disposiciones, no se verán de ninguna manera afectada o deteriorada.

La demora u omisión de la compañía, en exigir el estricto cumplimiento de estas políticas no puede bajo ninguna circunstancia interpretarse como renuncia a sus derechos.



Glosario

Para comprender el contenido de esta política hay algunas palabras y términos que deben ser explicadas:



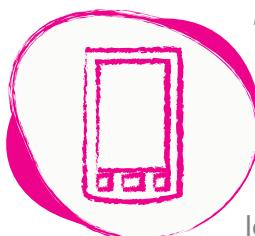
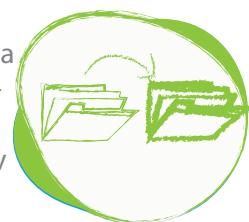
Estación de trabajo : equipo de cómputo destinado para la ejecución de tareas de automatizadas de usuario final. A esta agrupación partenecen computadores de escritorio y portátiles.

Antivirus: son programas que tienen como objetivo prevenir, detectar y/o eliminar los virus informáticos y programas maliciosos de los equipos de cómputo



Contraseña: se conoce también como clave. Es una forma de autentificación, que utiliza información secreta para controlar el acceso hacia nuestros equipos de trabajo o sistemas de información.

Copia de Respaldo: es proceso por el cual se duplica la información contenida en un dispositivo de almacenamiento masivo (memoria USB, disco duro de equipo de cómputo, tarjeta de almacenamiento, DVD entre otros) y se traslada a un segundo sitio de almacenamiento.



Dispositivos Móviles: son elementos de computo generalmente de tamaño reducido, con conexión permanente o intermitente a una red (con o sin Internet). Por lo general estos dispositivos pueden ser transportados en el bolsillo del propietario como localizadores, teléfonos celulares, PDA's (Asistentes Personales Digitales), tabletas, teléfonos celulares inteligentes, portátiles, terminales de radiofrecuencia, entre otros.



Mensajería instantánea: son un conjunto de programas que permite enviar y recibir mensajes en tiempo real con otros usuarios que se encuentran conectados a Internet. Los programas más utilizados de este tipo son Yahoo, Messenger, MSN Messenger, Google Talk, entre otros.



Modos: en SAP se refiere a una nueva ventana de la aplicación.



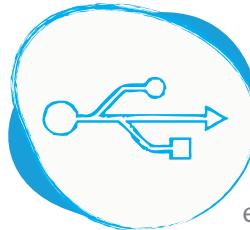
Outlook: es una aplicación que hace parte de la suite de Microsoft Office el cual se emplea para gestionar uno o varios buzones de correos electrónico.

OWA: (Outlook Web Access) permite visualizar los mensajes de correo electrónico desde el explorador de Internet mediante una dirección electrónica.

Papel Tapiz: Es una imagen que se coloca como fondo en el escritorio en las estaciones de trabajo.



Protector de pantalla: es un programa que contiene imágenes en movimiento, cuando un dispositivo no está siendo usado.



Salida USB: puertos de comunicación que poseen los equipos de cómputo para conectar dispositivos de almacenamiento u otro tipo de periféricos. Algunos ejemplos de estos dispositivos son ratones, teclados, escáneres, cámaras digitales, impresoras, discos duros externos.

SAP R/3: es un sistema de gestión de la empresa Alemana SAP que permite controlar todos los procesos que se llevan a cabo en una empresa, a través de módulos. Este sistema integra los procesos más importante de la cadena de valor interrelacionándolos y facilitando la posibilidad de intercambiar datos entre ellos.



SAP BW: es un sistema de la empresa Alemana SAP que permite realizar inteligencia de negocios (generar conocimiento y facilitar la toma de decisiones empresariales mediante el análisis de datos).

Software: son todos los componentes intangibles de una computadora, es decir, al conjunto de programas y procedimientos automatizados necesarios para hacer posible la realización de una tarea específica.

Software Espía: son aplicaciones que recopilan información sobre los datos que tenemos en nuestros dispositivos, donde la función más común, es recopilar información sobre el usuario y distribuirlo en Internet. Estas aplicaciones pueden ser instaladas en un equipo mediante un virus, por un correo electrónico o en la instalación de un programa aparentemente inofensivo.



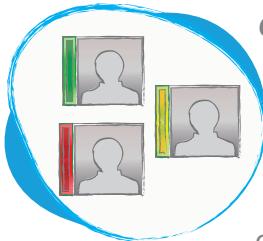
SPAM: son mensajes no solicitados enviados en cantidades masivas por Internet que perjudican nuestros dispositivos.



Virus: son programas informáticos que se ejecutan normalmente con el consentimiento de un usuario y que tiene la característica de ejecutar recursos, consumir memoria e incluso eliminar o destrozar la información que tenemos en nuestros dispositivos.



Modo de ahorro de energía: estado en el cual los elementos de cómputo cambian a un estado que desactiva gran parte de sus funciones y por consiguiente hace que su consumo de energía sea inferior.



Comunicaciones unificadas: sistema que integra las funcionalidades de presencia (saber el estado de un individuo en la red: conectado, ausente, ocupado), mensajería instantánea, video conferencia, reuniones en línea, tele conferencia, correo electrónico y colaboración compartiendo el escritorio en una sola aplicación o con la interrelación de varias aplicaciones.

Sistema de información: es un conjunto de elementos orientados al tratamiento y administración de datos e información.

Unidad segura: fracción del disco duro de una estación de trabajo que se encuentra cifrada por una clave para evitar accesos no autorizados a la información.



Reuniones en línea: encuentro virtual con personas que están conectadas a Internet mediante un software que se ejecuta en cada una de las estaciones de trabajo de los invitados.

Propiedad Intelectual: es la protección Legal que recae sobre toda creación del talento y del Intelecto humano, los procesos y resultados de la innovación, y todos los derechos existentes en cada momento bajo la normatividad que regula los derechos de autor, la propiedad industrial, secretos empresariales e industriales, el Know How, que puedan ahora o en el futuro estar vigentes en Colombia y en el mundo.

Servidores: computador de características especiales cuyo fin es "servir" de medio para realizar algún tipo de cómputo en una estación de trabajo. procesar correos, almacenar información, realizar cálculos, proporcionar un servicio.