ANEXO No1

POLITICA DE SEGURIDAD INFORMATICA

La política de seguridad informática adopta la gestión, el uso adecuado y la seguridad de la información, los activos informáticos y el ambiente tecnológico en general de CELT CONSULTORES S.A.S. Es deber de todos los empleados y contratistas que utilicen la información generada y custodiada por la entidad, conocerla en su totalidad.

LINEAMIENTOS GENERALES

- Todo empleado o contratista de la entidad es responsable por el manejo del espacio en disco en su equipo de trabajo, realizando revisiones periódicas y eliminación de archivos no necesarios.

- Todo empleado o contratista de la entidad es responsable de reportar oportunamente las debilidades e incidentes de seguridad que detecte o que sean de su conocimiento y de proteger el ingreso a los recursos informáticos a los cuales se les permite acceso mediante la utilización de contraseñas confidenciales; para tal fin, debe cerrar las sesiones activas al finalizar las tareas, y/o dejar los equipos bloqueados mediante protector de sesión protegido por contraseña.

- Para efectos de la conservación física de los equipos se debe prevenir interferencia eléctrica o magnética, riesgo de contaminación por alimentos, bebidas o golpes con objetos que perjudiquen o pongan en riesgo el funcionamiento de los mismos o deterioren la información almacenada en ellos.

- Todas las acciones realizadas bajo un nombre de usuario y contraseña de acceso, quedaran registradas y son responsabilidad del usuario titular.

- Ningún empleado o contratista está autorizado para efectuar algún tipo de intervención, reparación y/o modificación en un equipo a su cargo. El mantenimiento preventivo y correctivo debe ser realizado por técnicos.

Si para el cumplimiento de una actividad específica el empleado o contratista requiere temporalmente el uso de un elemento informático debe solicitarlo por medio del correo electrónico.

Todo empleado o contratista deberá devolver los activos informáticos que tiene a su cargo si por cualquier motive existe retiro ya sea definitivo o, temporal (mayor a tres meses), haciendo entrega formal de los activos a su cargo y claves de acceso.

Está prohibido intentar desinstalar o deshabilitar el software antivirus de los computadores por parte de los usuarios de la compañía. Si los usuarios sospechan la infección de un virus informático, deben vacunar sus archivos y verificar su eliminación mediante el software, de Antivirus, si el problema persiste se debe comunicar con el área de sistemas.

Está prohibido el uso de software ilegal so pena de acción disciplinaria. En caso de necesitar la instalación de algún software adicional, el empleado u contratista debe solicitarlo al área de sistemas.

No se debe descargar imágenes, sonidos y video, ya que pueden saturar el canal (ancho de banda) y disminuir la velocidad de transmisión.

Cada usuario es responsable de generar copia de seguridad de la información en el servidor de archivos que el área de sistemas disponga para ello. Para su solicitud se debe seguir los pasos enviados al correo electrónico.

Es responsabilidad de los usuarios la manipulación de los archivos compartidos, solo se permite archivos que estén directamente ligados a su función (no se permiten archivos personales).

Los recursos y servicios de Internet se usarán primordialmente para asuntos institucionales. El uso personal no debe interferir con la operación eficiente de los sistemas de la entidad, ni con los deberes y obligaciones de los empleados y/o contratistas establecidas en las funciones de su cargo.

- El uso de su cuenta de correo es con fines laborales y su uso es de carácter obligatorio, en ella llegara información oficial de conocimiento necesario para los empleados y contratistas de la entidad.

- Se requiere que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan a los sistemas informáticos.

- La cuenta y contraseña es personal e intransferible. No debe permitir que personas diferentes hagan uso de su cuenta de correo u otros accesos, esta debe poseer un mínimo de seis (6) caracteres y debe contener al menos una letra mayúscula, una letra minúscula y un número.

- Se prohíbe el uso e instalación de juegos, software pirata y pornografía en los computadores de la compañía.

DIRECTRICES GENERALES DEFINICIONES

Para los efectos de la presente política, se adoptarán las siguientes definiciones:

- Activo: Es todo aquel elemento que compone el proceso de la comunicación, desde hardware, software, datos y documentación.

- Aplicaciones o aplicativos: Las aplicaciones son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares

- Autenticación: Proceso utilizado entre un emisor y un receptor, con el fin de asegurar la integridad de los datos y proporcionar la autenticidad de los datos originales.

- Copia de respaldo: Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.

- Contenido: Todos tipos de información o datos que se divulga en la página web, entre los que se encuentran: textos, imágenes, fotos, logos, diseños, animaciones
- Clave de autenticación o Contraseñas: Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.

- Copyright: Derecho exclusivo de un autor o editor a explotar una obra física o digital, literaria, científica o artística.

- Dominio: Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red.

- Información personal: Es aquella suministrada por el usuario o el visitante para el registro o consulta de información, la cual incluye datos como nombre, identificaci6n, edad, genero, direcci6n, correo electrónico y teléfono, entre otros.
- Internet: Herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP-IP

- Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

- Medios de almacenamiento físico: Se considera como medio de almacenamiento físico las cintas, los discos extraíbles, los discos compactos.

- Nombres de Grupos: Seudónimos utilizados para la clasificación de conjuntos de computadoras dentro del dominio.

- Portal web: Es un sitio compuesto por varias páginas web, el cual, permite al usuario el fácil acceso a diferentes recursos y servicios que tienen relación con un mismo tema.
- Publicar: Es la acción de hacer visible un contenido o documento desde un portal o sitio web.

- Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

- Servidor: Computadora central en un sistema de red que provee servicios a otras computadoras

- Sistema Informático de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna forma mensajes de datos.

- Usuario: Es cualquier persona que utiliza una computadora o cualquier otro mecanismo para acceder y hacer uso de los sistemas informáticos de la entidad.

  Se considera usuario interno, todo empleado y contratista, que haga uso de los recursos informáticos de la entidad. A su vez, se considera usuario externo, todo ciudadano que haga uso de los recursos publicados mediante como el portal web y recursos de red a través de VPN mediante previa autorización.

ALCANCE

La política de seguridad informática adopta la gestión, el uso adecuado y la seguridad de la información, los activos informáticos y el ambiente tecnológico en general de la compañía. Esta política debe ser conocida y cumplida por empleados, contratistas y terceros que utilicen la información generada y custodiada por la entidad que hagan uso de los servicios informáticos de la misma.

DOCUMENTOS DE REFERENCIA - FUNDAMENTO LEGAL

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

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

Ley 1266 de 2008: "Por la cual se dictan las disposiciones generales del habeas data / se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"

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

Ley 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales".

Norma ISO 27001: Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestion de la Seguridad de la Información.

RESPONSABLES

AREA DE SISTEMAS

Responsable de aprobar las políticas de seguridad de la información aplicables al interior de la entidad, emitiendo las directrices y recomendaciones que considere pertinentes para uso y aplicación por parte de todos los usuarios. Debe realizar la verificación del cumplimiento de dichas directrices como mínimo en cada una de sus sesiones ordinarias, o de manera extraordinaria, cuando surja algún cambio significativo en la infraestructura tecnológica.

Responsable del inventario de equipos y su actualización según se establezca en las normas vigentes y de proporcionar los suministros que permitan la operación adecuada de los sistemas de información de la entidad por medio de los procesos contractuales necesarios tanto para la ampliación de la red como para su mantenimiento.

Deberá garantizar la divulgación y seguimiento de las políticas de seguridad de la información al interior de la compañía, estableciendo los procedimientos que permitan su operatividad y cumplimiento.

EMPLEADOS Y CONTRATISTAS

Todo empleado o contratista de la entidad es responsable de reportar oportunamente las debilidades e incidentes de seguridad que detecte o que sean de su conocimiento y de proteger el ingreso a los recursos informáticos a los cuales se les permite el acceso mediante la utilización de contraseñas confidenciales; para tal fin, debe cerrar las sesiones activas al finalizar las tareas, y/o dejar los equipos bloqueados mediante protector de sesión protegido por contraseña. De la misma forma es responsable por el manejo del espacio en disco en su equipo de trabajo, realizando revisiones periódicas y eliminación de archivos no necesarios.

LINEAMIENTOS GENERALES

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

Las actualizaciones, modificaciones o novedades en materia de seguridad se comunicarán mediante los medios tecnológicos habilitados para tal fin.

Todas las acciones realizadas bajo un nombre de usuario y contraseña de acceso, quedaran registradas y son responsabilidad del usuario titular.

La entidad deberá dar a conocer por medio de sus sistemas informáticos, la información y documentos que no contengan carácter reservado.

ASGNACION DE ROLES Y RESPONSABILDADES

El encargado del área de sistemas, conjunto a la gerencia establecerá los roles de usuario que se estimen pertinentes en cada uno de sus equipos y los niveles de operación.

CLASIFICACION DE LOS ROLES

Los roles asociados a cada servicio o sistema de información serán identificados y clasificados por su tipo y uso teniendo como base los siguientes criterios:

- Sistemas: Usuarios que por su actividad directa con los sistemas de información y de tecnología necesitan accesos especiales a los sistemas tecnológicos de la compañía.

- Internos: empleados o contratistas de la compañía que requieren diferentes niveles de acceso de acuerdo con los niveles de servicio asociados basados en sus funciones.

- Externos: Terceros con acceso a la red mediante VPN.

ADMINISTRACION DE ACTIVOS FISICOS

La administración de hardware conectado a la red y la atención de requerimientos de desarrollos y adecuaciones físicas, debe realizarse de acuerdo a lo establecido por el área de sistemas y la gerencia.

El cableado de energía eléctrica y de comunicaciones, deberá cumplir con los estándares vigentes según el reglamento interno de instalaciones eléctricas RETIE, RITEL Y norma de cableado EIAITIA 568. Cualquier cambio en las instalaciones eléctricas o ramales adicionales a los establecidos por la entidad debe hacerse presentando previa solicitud y con aprobación y supervisión técnica del área de sistemas.

El suministro de energía eléctrica deberá estar regulado a 110 voltios. Con polo a tierra, salvo especificación contraria del fabricante o proveedor de los equipos. Adicionalmente se debe contar con suministro de energía ininterrumpida (UPS) para asegurar la ejecución continua o el apagado regulado y sistemático.

Para efectos de la conservación física de los equipos se debe prevenir interferencia eléctrica o magnética, riesgo de contaminación por alimentos, bebidas o golpes con objetos que perjudiquen o pongan en riesgo el funcionamiento de los mismos o deterioren la información almacenada en ellos.

Se debe evitar colocar encima o cerca de los computadores ganchos, clips u otros elementos que puedan caer accidentalmente dentro del equipo. Adicionalmente se recomienda apagar la pantalla con el fin de ahorrar energía si se retira de su puesto de trabajo y apagar totalmente el equipo al finalizar la Jornada laboral.

MANTENIMIENTO PREVENTIVO Y CORRECTIVO

El área de sistemas deberá elaborar el cronograma de mantenimiento preventivo y correctivo el cual será notificado a las dependencias con mínimo una semana de antelación con el fin de asegurar la prestación del servicio a los usuarios. Adicionalmente, deberá informarse el nombre e identificación del personal autorizado para realizar las actividades de mantenimiento con el fin de evitar el riesgo de hurto y/o pérdida de equipos.

Toda solicitud de mantenimiento correctivo o asistencia técnica, debe realizarse siguiendo el Procedimiento, Cuando los equipos requieran de cambio de partes y no haya disponibilidad de las mismas, la compañía deberá provisionar al usuario afectado con un equipo de alterno destinado para tal fin como contingencia de acuerdo con la disponibilidad de equipos.

Ningún empleado o contratista está autorizado para efectuar algún tipo de intervención, reparación y/o modificación en un equipo a su cargo. El mantenimiento preventivo y correctivo debe ser realizado por personal del área sistemas, quienes deben contar con el entrenamiento y las herramientas necesarias.

RETIRO Y TRASLADO DE EQUIPOS

Para efectuar el traslado y/o retiro de equipos (incluidos la información y el software) por cambio del empleado responsable o cambio en la ubicación del equipo se debe comunicar al área de sistemas y a la gerencia.

Si para el cumplimiento de una actividad específica el empleado o contratista requiere temporalmente el uso de un elemento informático debe solicitarlo por medio del correo electrónico (sujeto a disponibilidad) a la gerencia quien autorizará y enviará una carta relacionando el equipo al personal de vigilancia y seguridad del edificio, quien a su vez registrara en la bitácora (libro de salida de elementos) con Nombre, cedula, fecha, hora, oficina que entrega y firma, para el proceso de retiro del equipo.

SEGURIDAD FISICA Y DEL ENTORNO

Las áreas para la gestión, almacenamiento y procesamiento de información de la compañía, (centro de cómputo y cuartos de comunicaciones), deben ser aseguradas y en lo posible monitoreadas con cámaras de video con el fin de prevenir o impedir accesos no autorizados, adulteración, perdida, consulta, danos e interferencia en el funcionamiento de los aplicativos e información de la entidad.

Todos los servidores y equipos de comunicaciones de voz y datos deben estar localizados en lugares seguros para prevenir el uso o acceso no autorizado. De igual forma, deberá contarse con protecciones físicas y ambientales para los activos críticos, incluyendo perímetros de seguridad, controles de acceso físicos, controles especiales en áreas de mayor sensibilidad, seguridad de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales de operación y sistemas de contención, detección y extinción de incendios.

SEGURIDAD PARA AREAS DE ACCESO RESTRINGIDO

Constituyen áreas de acceso restringido el Centro de Computo, los cuartos de potencia (planta eléctrica, Unidades de poder ininterrumpida UPS y cuartos de electricidad) y centros de cableado; por lo que solo el personal autorizado por la gerencia y el área de sistemas puede acceder a él. Este personal debe portal el carnet de la entidad que lo acredita como empleado o contratista del área en mención.

Toda persona ajena a la compañía que ingrese al Centro de Cómputo debe estar acompañada por un empleado de sistemas.

El centro de cómputo debe contar con equipos de vigilancia (cámaras) y sistemas de protección contra incendios, control de temperatura (Aire acondicionado) y sistema eléctrico de respaldo (UPS) de acuerdo con lo establecido en norma ISO 27001 estándar ANSI/BICSI 002.

No se permite ingerir alimentos o bebidas en las instalaciones del Centro de Cómputo.

Cualquier cambio que se realice en el Centro de Cómputo o centros de cableado, y que potencialmente afecte los sistemas de información de la entidad, debe estar previamente autorizado.

SEGURIDAD DE LA INFORMACION

Todo empleado o contratista deberá devolver los activos informáticos que tiene a su cargo si por cualquier motivo existe retiro ya sea definitivo o temporal (mayor a tres meses), haciendo entrega formal de los activos a su cargo y claves de acceso; De ser necesario instruir a su reemplazo en la utilización de la aplicación que opera, también debe solicitar la toma de la copia de respaldo del equipo al área de sistemas.

Adicionalmente es necesario garantizar que todos los empleados de la entidad, contratistas y terceros reciban formación adecuada en concientización y actualización sobre las políticas y los procedimientos de seguridad informática de la compañía según sea pertinente para sus funciones laborales.

Los sistemas de información de la entidad que contengan información reservada, se deben mantener con niveles de protección más estrictos con el fin de velar por su reserva.

PROTECCION CONTRA EL CODIGO MALICIOSO Y DESCARGABLES

La compañía deberá contar una herramienta contratada y actualizada que deberá realizar las siguientes tareas:

- Revisión periódica de las últimas definiciones de virus.
- Descarga de últimas actualizaciones de Internet o Corregir posibles alertas de virus.
- Todos los equipos de cómputo deben tener software de antivirus. Por lo tanto, todo equipo debe ser incluido dentro del dominio de la red "consultoria.local", para que se puedan ejercer los controles y apliquen las actualizaciones y detecciones correspondientes.
- El software de instalación en los servidores debe ser protegido contra escritura de tal manera que se prevenga su posible infección.
- Antes de distribuir datos a otros usuarios, se debe hacer una revisión a los mismos usando el software de Antivirus.

- Está prohibido intentar desinstalar y deshabilitar el software antivirus de las computadoras por parte de los usuarios de la entidad. Si los usuarios sospechan la infección de un virus informático, deben vacunar sus archivos y verificar su eliminación mediante el software de Antivirus, si el problema persiste se debe comunicar de inmediato el área de sistemas.
- Todo medio de almacenamiento, como discos duros removibles, USB y discos compactos que ingresen a la entidad, deben ser previamente revisados y/e vacunados como medida preventiva de evitar infección antes de su uso.
- Está prohibido el uso de software ilegal. En caso de necesitar la instalación de algún software adicional. El usuario responsable debe solicitarlo al área de sistemas.

GESTION DE LA PROVISION DE SERVICIOS POR TERCEROS

Los proveedores de servicio deberán cumplir las políticas de seguridad informática en cuanto a la reserva de la información de la entidad o lo que les aplique.

RESPALDO DE LOS SERVICIOS CENTRO DE CÓMPUTO

El área de sistemas realizará los procedimientos de copia, recuperación y pruebas de la información, estandarizando los medios y mecanismos para el registro de tareas y eventualidades de manera que se garantice la continuidad de prestación de servicios de la entidad y la atención oportuna de contingencias.

Los medios de almacenamiento físico y de red estarán instalados en el Centro de Cómputo, a los cuales tendrán acceso únicamente los empleados indicados por la gerencia para ser administrados.

En el caso de copias de respaldo a medios de almacenamiento físico, estas se harán mediante software especializado y/o programado.

Los usuarios de sistemas, encargados de la infraestructura tecnológica, deberán seguir los procedimientos de respaldo de la información establecidos internamente, en los que se especifican: periodicidad, tipo, jerarquía, generación y ubicación de las copias generadas.

Se considera como información a respaldar aquella que es exclusivamente de carácter corporativo. Ninguna información personal de los usuarios de la empresa será respaldada.

Este respaldo contempla los archivos compartidos de carácter documental, propios de la gestión encomendada por la misión de la entidad en su diaria marcha.

RESPALDO DE INFORMACION DE USUARIOS

Cada usuario es responsable de generar copia de seguridad de la información en el servidor de archivos que el área de sistemas asigne para tal fin.

El servicio de recursos y activos informáticos compartidos de la compañía esta disponible para todos los empleados y contratistas que lo requieran.

El área de sistemas, brindará las instrucciones y capacitaciones necesarias a los usuarios que requieran guardar información o compartir archivos en espacio del servidor.

Es responsabilidad de los usuarios la manipulación de los archivos compartidos, solo se permite archivos que estén directamente ligados a su función (no se permiten archivos personales), cualquier modificación a los mismos deberá atender los permisos otorgados y previamente solicitados.

Es responsabilidad de cada empleado y/o contratista identificar, clasificar y definir la información relevante a respaldar en los medios de almacenamiento autorizados, con el fin de mantener una copia original de los datos importantes y/o relevantes. Archivos no autorizados serán eliminados.

GESTION DE SEGURIDAD DE LAS REDES

El área de sistemas definirá controles para garantizar la seguridad de los datos y los servicios conectados a las redes de la entidad contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

- Establecer los procedimientos para la administración de los equipos remotos, incluyendo los equipos en las áreas restringidas.
- Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.
- Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.
- Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

MANIPULACION DE LOS SOPORTES DE COPIA DE INFORMACION

Se recomienda para el uso de medios informáticos removibles las siguientes acciones:

- En lo posible almacenar la información en los medios dispuestos para tal fin (carpetas compartidas)
- Eliminar de forma segura los contenidos no requeridos del medio reutilizable que ha de ser retirado o reutilizado en la entidad (discos duros, etc).
- Almacenar todos los medios en un ambiente seguro y protegido.

SALVAGUARDA DE LA INFORMACION

Los medios de almacenamiento transportados fuera de las instalaciones de entidad, deberán cumplir con los controles de seguridad establecidos para tal fin.

Toda la información que sea objeto de intercambio entre los diferentes sistemas de información estará controlada en cuanto a su acceso, envío, uso, almacenamiento y eliminación, de acuerdo con los controles de seguridad establecidos.

USO DE INTERNET

Las conexiones que acceden a Internet están protegidas por un Firewall, el cual está localizado entre la red privada y el proveedor de servicios de Internet, este controla (aplica seguridad) y supervisa las salidas hacia Internet.

Todos los usuarios conectados a red con equipos que posean las condiciones mínimas para el acceso a Internet, tendrán derecho a su instalación y podrán navegar conforme a los lineamientos establecidos por este documento.

Los recursos y servicios de Internet se usarán primordialmente para asuntos corporativos. El uso personal no debe interferir con la operación eficiente de los sistemas de la entidad, ni con los deberes y obligaciones de los empleados y/o contratistas establecidas en las funciones de su cargo.

El área de sistemas se reserva el derecho de bloquear sitios que se detecten como peligrosos (con contenidos no autorizados) para la seguridad de los recursos informáticos.

El uso indebido del canal de Internet por parte de un usuario puede ocasionar la suspensión.

No se puede descargar archivos o instalar programas de sitios web desconocidos o gratuitos.

El canal de internet será monitoreado periódicamente, para revisar el tráfico de paquetes, verificando el uso de este servicio.

El incumplimiento de las presentes normas acarreara las sanciones correspondientes según sea el caso.

USO DEL CORREO ELECTRONICO

Todo empleado de la compañía, dispondrá de una cuenta de correo electrónico activa.

La vigencia de la cuenta para contratistas comprende el periodo de contratación que inicia con la firma del acta de inicio y finaliza el último día de contratación, de acuerdo con la información del contrato.

Para casos excepcionales que un usuario, no empleado, requiera un correo corporativo lo deberá aprobar la gerencia tanto para su alta como baja.

El uso de su cuenta de correo es con fines laborales y su uso es de carácter obligatorio, en ella llegara información oficial de conocimiento necesario para los empleados y contratistas de la compañía.

Se prohíbe el uso de cuentas de correo gratuito con propósitos corporativos.

La cuenta y contraseña es personal e intransferible. No debe permitir que personas diferentes hagan uso de su cuenta de correo, esta debe poseer un mínimo de seis (6) caracteres y debe contener al menos una letra mayúscula, una letra minúscula y un número.

La compañía no se hace responsable por lo que se haga o diga en nombre de una cuenta particular y por lo tanto está prohibido el uso de cuentas por personas ajenas a su titular.

Cada cuenta tendrá un espacio de almacenamiento básico de 200 Mb. Cuando, debido a las necesidades de las funciones que desempeñe el empleado, requiera de su amplitud, deberá hacerse una solicitud al área de sistemas.

Es responsabilidad del empleado o contratista depurar su cuenta periódicamente siendo el único responsable de respaldar sus correos (Copia de respaldo).

El usuario debe leer diariamente su correo y borrar aquellos mensajes obsoletos, para liberar espacio en su buzón de correo.

El incumplimiento por parte del empleado o contratista de los lineamientos o el manejo de su cuenta, puede ocasionar la suspensión temporal del servicio y en caso de reincidencia, la suspensión del mismo y en un último caso la notificación a la gerencia.

Se considera como conductas de mal manejo:

- Exceder los servicios para los cuales se autorizó la cuenta.
- Enviar mensajes para la difusión de noticias, mensajes políticos, religiosos, correos sin identificar plenamente a su autor o autores o enviar anónimos.
- Difundir «cadenas» de mensajes que saturen el servicio entre otros problemas.
- Perturbar el trabajo de los demás enviando mensajes que puedan interferir con sus actividades laborales.
- Agredir o lesionar directa o indirectamente a otras personas.
- Suscribir las cuentas de correo institucional en servicios externos (comerciales) con fines no gubernamentales o afines a la misión corporativa.

No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca atractivos premios o temas provocativos, mucho menos si estos archivos tienen doble extensión.

No se debe confiar en los archivos gratuitos que se descargan de sitios web desconocidos, ya que son una potencial vía de propagación de virus.

De ninguna manera se deben ejecutar archivos de las siguientes características:

- Archivos que contienen más de un punto por ejemplo (diagrama.noticias.532.txt)
- Archivos que contienen alguna de las siguientes extensiones ejecutables (No permitidas): exe, vbs, pif, com, bat, dll, ocx

No contestar los mensajes SPAM, ni mensajes con falsos contenidos (Hoaxes), tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, bloqueo de cuentas bancarias, etc.

No responder correos donde soliciten ratificación o confirmación de contraseñas de cualquier cuenta o servicio que posea, el área de sistemas nunca solicitara por este medio dicha información.

El sobrepaso de temario de archivos adjuntos por encima de 200MB, puede provocar que los destinatarios no reciban el mensaje. Es importante tomar en consideración el tamaño de los archivos enviados como adjuntos en el correo (attachments). Si se envían comprimidos, se ahorra tiempo de conexión y se evita saturar la red.

Procure colocar siempre en la linea de "Asunto:", un contenido conciso que tenga significado para el destinatario y le motive a leer el contenido del correo.

LISTAS DE CORREO

Cada usuario puede solicitar la creación de listas de correo al área de sistemas donde se especifique el nombre de la lista, la justificación, el responsable de su solicitud y contenido, el nombre de los integrantes de la lista con sus respectivos buzones de correo y el nombre del jefe o directivo que aprueba.

Las listas de correo que incluyen los usuarios internos y/o externos de la entidad, debe ser moderada y aprobada por la gerencia.

SEGURIDAD DE LAS CONTRASENAS

Se requiere que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas temporales, que se asignan cuando los usuarios olvidan su contraseña, solo debe suministrarse una vez identificado el usuario.

Para prevenir los ataques contra los intentos de adivinar la clave, la cuenta podrá ser desactivada después tres (3) intentos erróneos consecutivos.

Solamente puede solicitar cambio de contraseña el empleado al cual pertenece dicho usuario o el jefe inmediato mediante comunicación con el área de sistemas.

Los sistemas deberán estar configurados de tal manera que requieran contraseñitas fuertes, no repetibles en un periodo de tiempo o en cambios anteriores, bloqueo de cuentas y solicitud de cambio de tiempo después de cumplido un periodo de tiempo.

Se recomienda cambiar las contraseñas si se sospecha que han sido empleadas por otras personas, solicitándolo al área de sistemas.

Bajo ninguna circunstancia las contraseñas de los usuarios deben ser compartidas o reveladas a otra persona porque de lo contrario el usuario está asumiendo la responsabilidad de las acciones que la otra persona toma con su contraseña.

Los administradores podrán restablecer las contraseñas solamente en el evento que el usuario haya olvidado su contraseña, no sin antes haber verificado su identidad.

CONTRASEÑAS DE ADMINISTRACION

Las contraseñitas de administración de servicios (aplicaciones, bases de datos, dispositivos, servidores, controles de acceso, programas especiales y gestores), deben ser guardadas en documento por el encargado del área de sistemas y solo serán entregadas en momentos de aplicación de las contingencias o para propósitos específicos.

Las contraseñas de administración deben ser cambiadas cuando se haga uso de estas de manera regular y deben cumplir con todos los demás lineamientos generales de políticas de contraseñas establecidos en este documento.

Para las contraseñas administrativas se recomienda una longitud no menor a 8 caracteres.

CONTRASEÑAS DE ADMINISTRADOR LOCAL

La contraseña de administrador local de una estación de trabajo nunca caduca. Esta contraseña es general para todas las estaciones de trabajo y se usa para efectos de Soporte en cada una de estas estaciones.

Se recomienda la duplicidad de cuentas administrativas locales para estaciones de trabajo, La cuenta "Administrador" solo podrá definir el Administrador de la Red, la otra cuenta puede ser modificada y manejada por los grupos de soporte de la red.

PROPIEDAD INTELECTUAL

Se implementarán procedimientos para garantizar el cumplimiento de las normas de propiedad intelectual. El incumplimiento de las normas de propiedad intelectual puede derivar en sanciones penales, fiscales y disciplinarias.

Cuando el personal de soporte técnico encuentre programas instalados en los equipos, sin el respectivo licenciamiento, procederá con la desinstalación de los mismos, efectuando el registro correspondiente e informando, según sea el caso, a la gerencia.

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

El área de sistemas es la única dependencia autorizada para realizar copia de seguridad del software original.

Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización con lleva a las sanciones administrativas y legales pertinentes.

El software adquirido por la compañía, no puede ser copiado o suministrado a terceros.

Se prohíbe el uso e instalación de juegos, software pirata y pornografía en los computadores de la compañía.

Los empleados, contratistas o terceros responsables de la publicación de la información en el sitio WEB de la compañía, deberán atender el cumplimiento de las normas en materia de propiedad.

COMUNICACION Y SOCIALIZACION DE LAS POLITICAS

Todo empleado o contratista que ingrese a prestar funciones o servicios deberá recibir capacitación sobre la política de seguridad de la información y demás aplicaciones que dispone la entidad en el momento de su inducción, durante la cual se darán a conocer las obligaciones para con los usuarios y las sanciones que puede acarrear su incumplimiento y los documentos en las que están consignadas.

La inducción en el puesto de trabajo referida al uso de las herramientas tecnológicas será impartida por el área de sistemas, previa concertación de hora y lugar.

La gerencia remitirá al área de sistemas la relación de aquellos usuarios que requieran inducción sobre uso de los sistemas de información.

SUPERVISION y AUDITORIA

La gerencia podrá acceder a toda la infraestructura tecnológica de la entidad para realizar inspección de todos los dispositivos informáticos que se conectan a la red para propósitos de auditoria, resolución de problemas o para investigar violaciones a las políticas establecidas toda vez que lo necesite y sin previo aviso.