MANUAL DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCION

Para KCP DYNAMICS BOGOTA SL es claro que los datos de información personal administrados y tratados en el desarrollo de su objeto social son un componente importante, es por eso que ha decidido adoptar el siguiente Manual con el cual se busque asegurar la protección de la información de una forma adecuada, con el fin de dar pleno cumplimiento a lo dispuesto por La Constitución Política y a la Ley 1581 de 2012.

Este documento detalla las normas de seguridad definidas por KCP DYNAMICS BOGOTA SL con el propósito de dar a conocer a sus funcionarios los aspectos que deben considerarse y que serán los lineamientos para la implementación de controles, procedimientos y directrices, todo esto teniendo en cuenta que el compromiso de mantener la seguridad de la información es responsabilidad de todos los funcionarios de la empresa.

OBJETIVO

El objetivo de este documento es establecer los lineamientos en seguridad de la información de KCP DYNAMICS BOGOTA SL en concordancia con el Marco Legal establecido Ley 1581 de 2012 y sus decretos reglamentarios o posteriores que la deroguen o modifiquen.

ALCANCE

El manual de Seguridad en la Información aplica para toda la organización Directivos, Funcionarios, clientes y Terceros (Contratistas y Proveedores) que laboren o tengan una relación con KCP DYNAMICS BOGOTA SL.

DEFINICIONES

Autorización: Consentimiento previo, expreso e informado del titular de los datos personales para llevar a cabo el tratamiento de datos personales.

Activos de información: Corresponde a la información que para la entidad tiene significado y valor y debe ser protegida tales como: bases de datos, documentación, manuales de usuarios, planes de continuidad y que reposan en medio físico o magnético (transmitida por algún medio electrónico, almacenada en equipos de cómputo, servidores, almacenada en la nube, memorias, dispositivos móviles, etc), microfilmada o por cualquier otro medio de almacenamiento.

Base de datos: Conjunto organizado de datos personales que sea objeto de Tratamiento.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables.

Encargado del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realiza el tratamiento de datos personales por cuenta del responsable del tratamiento.

Responsable del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decide sobre la base de datos y/o el Tratamiento de los datos.

Titular: Persona natural cuyos datos personales sean objeto de Tratamiento.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES

KCP DYNAMICS BOGOTA SL aplicará los principios que se enuncian a continuación los cuales están relacionados con la protección de Datos Personales.

Principio de Legalidad: La actividad del tratamiento de datos, debe sujetarse a lo establecido en la Ley 1581 de 2012 y las demás disposiciones que la regulen.

Principio de Finalidad: El tratamiento de Datos personales que KCP DYNAMICS BOGOTA SL realiza, lo hace cumpliendo con lo descrito en la Constitución Política, la Ley 1581 de 2012 y los Decretos que la complementan.

Principio de Libertad: KCP DYNAMICS BOGOTA SL solo puede ejercer el tratamiento de los datos de los cuales se tenga del titular la autorización o consentimiento de manera previa, expresa o informada.

Principio de Veracidad o Calidad: La información sujeta al tratamiento debe ser veraz, completa y exacta, actualizada, comprobable y comprensible. Está prohibido el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Principio de Transparencia: KCP DYNAMICS BOGOTA SL la garantiza a los titulares de la Información que en cualquier momento y sin restricciones podrán obtener la información de los datos que le conciernen.

Principio de acceso y circulación restringida: El tratamiento de los datos personales solo podrá hacerse por personas autorizadas por el titular y/o personas previstas cuando una disposición legal así lo permita. Los datos personales no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la ley 1581 de 2012.

Principio de Seguridad: El manejo de la información se deberá hacer por parte del encargado utilizando las medidas técnicas, humanas y administrativas que sean necesarias para otorgar la seguridad de los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Principio de confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar el suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la Ley 1581 de 2012 y en los términos de la misma.

Principio de temporalidad o caducidad: El periodo de conservación de los datos personales, será el necesario para alcanzar la finalidad para la cual se han recolectado.

SEGURIDAD DE LA INFORMACION

Con este manual se busca dar a conocer a los funcionarios de KCP DYNAMICS BOGOTA SL y a los titulares de la información, los lineamientos y directrices relacionados con la seguridad del manejo de la información.

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

NORMAS DE SEGURIDAD DE LA EMPRESA

NORMA DE INGRESO A LA EMPRESA

Los funcionarios de KCP DYNAMICS BOGOTA SL, están identificados con su carné empresarial y el acceso a la oficina se realizará a través de control biométrico (huella dactilar o clave).

En caso de olvido de la clave de acceso, el funcionario deberá comunicarse en forma inmediata al área de Recursos Humanos o al área Administrativa para solicitar una nueva.

En el evento de retiro de un funcionario de la empresa, el área de recursos – humanos debe validar la entrega del carné y proceder a la desactivación del usuario y de la clave de acceso o huella.

Para el acceso de clientes y proveedores, estas visitas deben anunciarse en la recepción del Edificio, quienes solicitarán a KCP la autorización de ingreso a las oficinas, los datos de los visitantes quedan registrados en una planilla.

NORMA DE ACCESO A AREAS AL INTERIOR DE LA EMPRESA

Aplica para los empleados como para terceros los controles de acceso a las diferentes áreas, dentro de las cuales están las de acceso restringido.

Únicamente el personal de KCP DYNAMICS BOGOTA SL que esté autorizado puede acceder a las áreas restringidas de acuerdo a las funciones que desarrolle.

En el evento que funcionarios de otras áreas o terceros que lo requieran para desarrollar una actividad no habitual, deben obtener autorización del Responsable de esta área y seguir las instrucciones y procedimientos que en esta están establecidos.

NORMA MANEJO LLAVES

El Área Administrativa debe establecer los procesos y las responsabilidades del manejo de llaves físicas. Dentro de estas están aquellas que permiten el ingreso a las oficinas y al centro de cómputo, las llaves que corresponden a los archivadores o muebles en donde se conserva información considerada como critica para la compañía y se custodian en el Área administrativa.

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

NORMA DE SEGURIDAD DE LOS ACTIVOS DE INFORMACION

Se deben identificar los activos de información que se generan al interior de KCP DYNAMICS BOGOTA SL, los medios y lugares de almacenamiento y los tipos de formatos.

Para identificar la información se deben tener en cuenta los diferentes tipos de activos de la información que intervienen y apoyan en los procesos como soportes físicos: Contratos, propuestas, manuales, memorandos, comprobantes contables, reportes del sistema, requerimientos, facturas entre otros.

Se debe identificar el tipo de información que genera el sistema bien sea financiera, operativa, de cumplimiento normativo, gerencial.

Establecer los lugares y medios de almacenamiento, especificando si la información se encuentra en medio físico como archivadores, escritorios, en medios electrónicos como en discos duros, servidores, en la nube.

Identificar los responsables del manejo y la custodia de esta información especificando el Cargo y la persona.

Clasificación de la información: Independiente de su medio de almacenamiento la información que maneja KCP DYNAMICS BOGOTA SL debe ser clasificada en función de su criticidad, de sus requisitos legales, su confidencialidad, esta se clasificará en:

Información Restringida: Es información muy importante para la compañía, la cual solo puede ser accedida por los directivos y encargados del área, estos últimos para el cumplimiento de sus funciones. Por su nivel de sensibilidad tiene un alto grado de seguridad.

Información Interna: Información disponible para los empleados de la empresa

Información Pública: Información disponible para cualquier persona interesada, no tiene el carácter de confidencial**.**

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

NORMAS MANEJO ADECUADO DE LOS ELEMENTOS DE LA INFORMACION

Todos los funcionarios de KCP DYNAMICS BOGOTA SL son responsables de cumplir el manual y las políticas de Seguridad de la información y al interior de cada área deben implementar los controles adecuados para salvaguardar la información a su cargo y también aquella a la que tengan acceso según sus funciones.

El personal de KCP DYNAMICS BOGOTA SL debe conservar su escritorio libre de información y/o documentación propia de la compañía, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

En los tableros que se ubicaron en las oficinas y salas de juntas, estos no deben tener información clasificada como restringida, al culminar las reuniones, esta información debe ser borrada y el tablero preferiblemente permanecer limpio.

No se debe tener archivos físicos debajo de los escritorios, estos deben reposar en las áreas designadas para esto.

Cuando un funcionario por diferentes razones se ausente de su puesto de trabajo debe: bloquear con el protector de pantalla el computador asignado, guardar en su escritorio bajo llave la información que esté trabajando, los medios de autenticación que utilice como tokens, dispositivos de almacenamiento y no dejar las llaves a la vista.

Se debe evitar realizar impresiones en papel reciclado que contenga información restringida de la compañía, en el evento que esto ocurra recoger de inmediato la impresión. Y no se deben dejar en el escritorio sin custodia.

No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

Es responsabilidad del personal de KCP DYNAMICS BOGOTA SL el uso de medios de almacenamiento, tales como discos externos, memorias USB, micro USB, etc., los cuales no deben estar desatendidos bajo circunstancia alguna.

NORMAS USO DE INTERNET

El servicio de internet suministrado por KCP DYNAMICS BOGOTA SL a los usuarios es exclusivamente para fines laborales.

No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de KCP DYNAMICS BOGOTA SL o que representen peligro para la Compañía como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por KCP DYNAMICS BOGOTA SL.

NORMAS DE SEGURIDAD DEL CENTRO DE DATOS Y CENTROS DE CABLEADO

El ingreso de personal no autorizado al centro de datos está prohibido. Este cuenta con una llave de seguridad.

En las instalaciones del centro de datos o centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.

En el centro de datos y cableado el acceso a las cajas de control eléctrico deben permanecer libres de cualquier obstáculo. Igualmente, todo elemento diferente a equipos de cómputo, telecomunicaciones y servidores deberán estar ubicados en un sitio dispuesto para tal fin.

Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro de datos.

NORMAS USO DE CORREO ELECTRONICO

Los usuarios no deben usar las cuentas de correo asignadas a otras personas, ni recibir mensajes en cuentas de otros. En tiempos prolongados de ausencia como vacaciones, los usuarios deberán activar la respuesta automática o bien de ser necesario con autorización del jefe inmediato autorizar la redirección a una cuenta de correo interno. Está prohibido redireccionar a cuentas privadas o personales.

Periódicamente cada usuario deberá cambiar la contraseña como medida de seguridad, a través del sistema WebMail.

Toda información enviada por correo electrónico es considerada confidencial y de propiedad de KCP DYNAMICS BOGOTA SL por lo tanto cada usuario deberá tomar las medidas que considere pertinentes para mantener la reserva de la misma.

Está prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

Está prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar comunicaciones electrónicas.

KCP IT, se reserva el derecho a acceder y revelar información de comunicaciones enviadas o recibidas por correo electrónico para cualquier propósito de personal que ha comprometido la seguridad, confidencialidad o acciones no permitidas.

Cada usuario es responsable de darle buen uso a la cuenta de correo corporativa, evitando prácticas que puedan comprometer la seguridad de la información.

La cuenta de correo corporativa solo puede ser usada para fines laborales ajustados a las funciones que realiza el usuario. Por ningún motivo la cuenta de correo corporativa podrá ser incluida en listas de boletines, publicidad, hacer parte de cadenas spam, re-envío de correo masivo, o cualquier otro uso de carácter personal.

No está autorizado el envío de correos con contenido que atenten contra la integridad y dignidad de las personas o el buen nombre de la compañía.

La creación de nuevas cuentas de correo, así como de aquellas cuentas que deban ser deshabilitadas por retiro de personal, deberá ser solicitada por el área de recursos humanos a través del sistema para gestión de requerimientos designado por KCP.IT

Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos o ejecutarlos y se debe reenviar el correo a la cuenta kcp.it@kcpdynamics.com con la frase “correo sospechoso” en el asunto.

Las cuentas de correo electrónico son propiedad de KCP DYNAMICS BOGOTA SL, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con la Compañía, ya sea como personal de planta o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la Compañía y no debe utilizarse para ningún otro fin.

Los correos electrónicos enviados deben estar acompañados de la siguiente nota al final del mensaje:

El contenido de este mensaje y sus anexos son de propiedad de KCP DYNAMICS BOGOTA SL, es únicamente para el uso del destinatario ya que puede contener información privada y/o confidencial, la cual no es de carácter público. Si usted no es el destinatario, se informa que cualquier uso, difusión, distribución o copiado de esta comunicación está prohibido. Cualquier revisión, retransmisión, diseminación o uso del mismo, así como cualquier acción que se tome respecto a la información contenida, por personas o entidades diferentes al propósito original de la misma es ilegal.
Si usted es el destinatario, le solicitamos dar un manejo adecuado de la información; de presentarse cualquier suceso anómalo, por favor informarlo al correo kcp.it@kcpdynamics.com

NORMAS PARA USO DE DISPOSITIVOS MOVILES.

Los dispositivos personales tales como móviles, tablets, teléfonos inteligentes entre otros no tienen permitido el uso de los recursos de la red interna y wifi, al igual que el uso de internet de la compañía.

Solo es permitida la configuración de la cuenta de correo corporativa en el dispositivo si y solo si el dispositivo cumple con los requisitos técnicos de conexión.

El usuario asume toda responsabilidad por el manejo de información y confidencialidad. En caso de pérdida o hurto el usuario debe informar inmediatamente para proceder con el bloqueo de la cuenta de correo corporativo.

NORMAS PARA EL USO DE CONEXIONES REMOTAS.

El acceso remoto para usuarios de KCP DYNAMICS BOGOTA SL está permitido siempre y cuando sus labores y funciones requieran el uso de estos recursos.

El área de IT es quien determina los métodos y controles de seguridad para acceso del personal autorizado de KCP DYNAMICS BOGOTA SL.

El área de IT debe verificar la efectividad de los controles de acceso aplicados a conexiones remotas.

Los usuarios KCP DYNAMICS BOGOTA SL que tengan autorización para uso de conexiones remotas deberán acceder a estos siempre desde el equipo de cómputo asignado por el área de IT, y que se encuentre registrado dentro del inventario de activos, nunca desde computadores públicos.

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

NORMAS POR RESPONSABILIDAD EN MANEJO DE ACTIVOS DE INFORMACION EN MEDIOS DE ALMACENAMIENTO.

El área IT de KCP DYNAMICS BOGOTA SL es responsable por la administración de los recursos tecnológicos representados en infraestructura de redes, cuarto de datos, cuarto de cableado, servidores, y el relacionado con servicios locales, así como de la gestión de recursos alojados en la nube.

El área de IT de KCP DYNAMICS BOGOTA SL tiene bajo su responsabilidad el alistamiento de portátiles que serán asignados o transferidos al personal. Del mismo modo deberá velar por mantener un inventario de equipos informáticos actualizado.

El área de IT será responsable de generar las copias de seguridad pertinentes contenidas en los equipos de cómputo entregados por funcionarios que han sido retirados de la compañía, cuando el responsable del Área de Recurso y Talento Humano ha realizado solicitud formal.

Todo recurso asignado a los usuarios de KCP DYNAMICS BOGOTA SL deberá ser utilizado de forma ética y en cumplimiento de las leyes y reglamentos vigentes, para no incurrir en daños o pérdidas que perjudiquen la operación y prestigio de la compañía.

Los recursos tecnológicos puestos a disposición de los usuarios en KCP DYNAMICS BOGOTA SL son con el único fin de ejecutar una labor eficiente, por lo tanto, no podrán ser utilizados para fines personales o ajenos a este.

El uso de equipos de cómputo y dispositivos móviles personales no está permitido para desempeñar actividades laborales.

Ningún usuario tiene permitido instalar o utilizar software no autorizado o de su propiedad en los equipos de trabajo.

Toda acción que ejerza detrimento, vulneración de la seguridad perimetral, sobre la red interna, y saturación en el canal de internet por parte de los usuarios tendrá sanción.

Cuando un usuario entre en proceso de desvinculación o cambio de actividades, deberá entregar los equipos y accesorios de cómputo recibidos en asignación, adjuntando el formato correspondiente de paz y salvo para ser radicado en la dirección de recursos humanos.

NORMAS PARA EL USO DE TOKENS DE SEGURIDAD

El área de IT no tiene bajo su responsabilidad la administración de tokens de seguridad de terceros, tales como tokens para acceso a entidades financieras, o VPN de clientes especiales.
El usuario que haya recibido un token de seguridad de un tercero es quien deberá asumir el compromiso y responder por el buen uso de estos frente a la entidad emisora. El uso de estos

dispositivos es exclusivo, personal e intransferible por lo que el usuario asumirá toda responsabilidad por la pérdida de estos.

El almacenamiento de tokens debe efectuarse bajo estrictas medidas de seguridad en la tula o sobre asignado para cada token, dentro de escritorio con llave o lockers de tal forma que se mantengan fuera del alcance de terceros no autorizados.

El usuario deberá notificar por escrito a la entidad emisora en caso de pérdida, robo, mal funcionamiento o caducidad para que desde allí procedan con la respectiva reposición.

NORMAS DE ACCESO A REDES Y RECURSOS DE RED

EL área de IT debe establecer un procedimiento de autorización y control para proteger el acceso a las redes de datos y recursos de la red interna de KCP DYNAMICS BOGOTA SL.

El área de IT debe asegurar que las redes inalámbricas de la compañía cuenten con mecanismos de autenticación óptimos para impedir accesos no autorizados.

El área de IT suministrará y establecerá los protocolos de acceso a internet para invitados.

NORMAS DE CONTROL Y ACCESO A USUARIOS

El área de IT determinará los mecanismos de validación para acceso de usuarios. Los intentos no autorizados para saltar o burlar los elementos y/o esquemas de seguridad, el uso de sistemas de red o el ordenador asignado por KCP Dynamics para otros fines o los ya previstos, para denegar el servicio a los usuarios autorizados para acceder, obtener, alterar, dañar o destruir la información, o de otra manera interfieran con la red o su funcionamiento están prohibidas.

La evidencia de este tipo de actos puede ser revelada a las autoridades policiales y resultar en un proceso penal bajo todas las leyes penales aplicables.

Otras acciones prohibidas incluidas, pero que no se limitan a lo siguiente:

Los intentos por eludir los procedimientos de autenticación o seguridad de cualquier servidor, red, componente de la red, o cuenta de acceso a los datos, cuentas o servicios que el usuario no tiene permiso o autorización de acceso expresamente.

El uso de la red o sistemas de una manera que agote el espacio en disco, procesadores, u otros recursos del sistema más allá de lo permitido por el tipo específico de cuenta o hacer intentos

deliberados de interferir con una empresa, sobrecargar un servicio, o intentar desactivar un host.

Transmitir a sabiendas virus informáticos, gusanos, troyanos, robots, o cualquier otro código de programación destructiva con la intención de interferir en el funcionamiento, función o uso de cualquier servicio o sistema.

La manipulación o el intento de alterar las secuencias de comandos que se presentan en las páginas Web o configurar una página Web para actuar maliciosamente contra los usuarios que visitan la página web.

Otro uso no autorizado, incluyendo, pero no limitado a, estafar a otros en la liberación de sus contraseñas, ataques de denegación de servicio ataques (envío de paquetes con un tamaño de paquete ilegal, bombardeo de correo, inundaciones UDP, saturación de líneas de comunicación, entreabierta la conexión TCP inundaciones, etc.).

Contraseña "cracking". El uso de cualquier programa de ordenador y / o el dispositivo para interceptar o decodificar contraseñas o información de control de acceso similar es prohibido.

Escaneado en red. Tentativas de análisis, sonda, o equipos de prueba en la red de KCP Dynamics utilizando analizadores de puertos o software de búsqueda de red (incluyendo analizadores de paquetes) con la intención de evaluar, detectar agujeros, o de otra manera violar la seguridad está prohibido, excepto por personal KCP.IT que son designados para ejercer funciones de trabajo específicas.

Registros de actividad. Los usuarios deben ser conscientes que la mayoría de los sistemas de TI de forma rutinaria registran las acciones en la sesión del usuario por una variedad de razones, incluyendo la recuperación del sistema, solución de problemas, informes de uso, y la planificación de los recursos.

NORMAS DE SEGURIDAD DE REDES

Conexiones no compartidas. Una conexión de red suministrada por KCP Dynamics es exclusivamente para el uso individual del trabajador asignado a esa conexión. Las conexiones no se pueden compartir entre varios usuarios. Los usuarios de la red de KCP Dynamics no podrán

utilizar mecanismos (ya sea hardware o software) para proporcionar conectividad de red a otras personas no relacionadas con KCP Dynamics.

Responsabilidad de manejo en la cuenta personal. El uso de las redes y sistemas de información de KCP Dynamics, que requieren de una cuenta de usuario expedida por el Departamento de Tecnología de KCP, para la concesión de acceso a un recurso en particular. Los usuarios son responsables de mantener la seguridad de sus propias cuentas y contraseñas. Las cuentas y las contraseñas son asignadas a usuarios individuales y no deben ser compartidos con otra persona sin la autorización de KCP.IT o el administrador del sistema. Toda cuenta de usuario para inicio de sesión en el computador asignado suministrado por KCP Dynamics, queda bajo responsabilidad de la persona quien asume la tenencia de ese activo y es igualmente responsable por el uso del equipo y de las conexiones de red, de esta forma asumirá la responsabilidad por cualquier violación que se produzca y en la cual se vea implicado su ordenador o conexión de red.

Sistemas de acceso restringido. El acceso a los equipos de la red, servidores y / o programas de aplicación está restringida sobre una base "necesidad de conocer", de conformidad con las directrices KCP.IT y / o las políticas corporativas. Los usuarios tienen derecho a acceder sólo los recursos de TI que sean compatibles con su nivel de autorización. El acceso no autorizado o intento de acceso a los recursos o datos restringidos pueden constituir robo de información. El empleado que sea sorprendido o se le compruebe estar involucrado será sancionado con medidas disciplinarias y / o acciones legales.

Seguridad en el manejo de la contraseña. Es obligatorio que las cuentas de usuario se mantengan seguras, manteniendo en secreto las contraseñas, y realizando el cambio de contraseña con frecuencia. Los usuarios deben elegir contraseñas que protejan a sus cuentas del uso no autorizado, y que no resulten fáciles de adivinar. Si las contraseñas son configuradas para expirar de forma automática (por ejemplo, una vez al mes), los usuarios no deben intentar alterar y/o evitar estos esquemas de seguridad.

Administración remota. KCP.IT llevará a cabo de forma rutinaria funciones de administración de equipos remotos, incluyendo la distribución de actualizaciones de software y de ver o tomar el control de sistemas distribuidos para ayudar a los usuarios con problemas. Las siguientes actividades pueden interferir con la capacidad del KCP.IT para llevar a cabo la gestión remota, y por lo tanto están prohibidas.

- Modificación o supresión de la cuenta local para administración del equipo portátil y/o contraseña.
- Modificación del nombre de la estación de trabajo vs nombre NetBIOS.
- Sacar una estación de trabajo del dominio asignado por KCP.IT.
- Volver a instalar el sistema operativo de una estación de trabajo o equipo portátil.
- La instalación de un sistema operativo en la estación de trabajo y/o equipo portátil diferente al suministrado por KCP.IT.

- La instalación de cualquier software de propiedad personal con o sin licencia.
- Cualquier manipulación no autorizada sobre el software instalado por KCP Dynamics, incluyendo, pero no limitado a:

  a. La eliminación o supresión de cualquier aplicación de software;
  b. Modificaciones a cualquier aplicación, herramientas, configuraciones al sistema operativo o servicios, y
  c. Modificaciones a la configuración de la red, configuraciones de máquina, configuraciones en la red Wifi, VPN, nombres de dispositivos y configuraciones al dominio y dispositivos de administración.

Prohibiciones Generales

- Utilización encubierta. Los usuarios no deben ocultar su identidad al utilizar los recursos de TI, excepto cuando la opción de acceso anónimo esté expresamente autorizada. Los usuarios también tienen prohibido pasar por o Suplantar la identidad o de otra manera utilizando una identidad falsa.
- Ordenadores personales de propiedad privada. Los empleados tienen prohibido fijar los ordenadores personales de propiedad privada u otros recursos de TI a la red de KCP Dynamics salvo autorización expresa de KCP.IT.
- Infracción de copyright. Los hechos de violación a los derechos de autor, incluyendo la oferta de programas de ordenador pirateados, o proporcionar enlaces a este tipo de programas, están prohibidas. También se prohíbe el suministro de información utilizado para eludir los dispositivos de protección contra copia instalados por el fabricante, incluyendo números de serie o números de registro para los programas de software, a cualquier persona que no sea el usuario con licencia del software.

RESUMEN

Los intentos no autorizados para derrotar o burlar los elementos de seguridad, el uso de sistemas de red o el ordenador de KCP Dynamics para otros fines que los previstos, para denegar el servicio a los usuarios autorizados para acceder, obtener, alterar, dañar o destruir la información, o de otra manera interfieran con la red o su funcionamiento están prohibidas. La evidencia de este tipo de actos puede ser revelada a las autoridades de policía, judiciales y a la Fiscalía y dar lugar a un proceso penal bajo las leyes vigentes que apliquen. Los empleados que se dediquen a actividades prohibidas en contravía de esta política y normas y / o leyes penales aplicables estarán sujetos a medidas disciplinarias que pueden incluir el despido.