La información es un activo crítico de Manpower Inc., sus subsidiarias y empresas asociadas.

Dada la importancia de esta información, se deben tomar las medidas adecuadas razonables

para asegurar la confidencialidad, integridad y disponibilidad de la misma.

La protección de archivos computarizados almacenados en redes corporativas ha sido

tradicionalmente el foco principal de los especialistas en seguridad. Sin embargo, la

información almacenada en una computadora personal, PDA u otro dispositivo portátil, o bien

en un CD, una memoria extraíble (flash) u otros medios (incluyendo papel) también debe ser

protegida contra daños o acceso o divulgación no autorizados. De igual modo, se deben

tomar medidas de protección cuando la información es transmitida vía correo electrónico, fax u

otros medios.

Los controles de seguridad adecuados son esenciales para mantener el alto nivel de confianza

que han depositado en nosotros nuestros clientes, socios comerciales, empleados temporales,

candidatos y empleados. Esta confianza puede ser seriamente dañada por apenas un simple

incidente. Intrusiones de hackers, ataques a las páginas Web, o publicación de información

confidencial podrían hacer que nuestros clientes perdieran confianza en nosotros y nuestra

reputación se viera degradada. La confianza que nuestros clientes, socios comerciales y otros

tienen en nosotros es una ventaja competitiva que debe ser alimentada y preservada.

Proteger la privacidad es un objetivo primordial del programa de Manpower de Seguridad de la

Información – pero no puede haber privacidad sin seguridad. El objetivo fundamental de

Manpower en términos de seguridad es ofrecer un nivel de protección que alcance o exceda

las mejores prácticas de nuestra industria.

Propósito

Estas Políticas para los empleados sobre el uso de los recursos informáticos proporcionan las

medidas básicas de control que todas las entidades comerciales de Manpower deben

implementar. Tales medidas son requeridas para reducir la probabilidad de problemas como

fraude, desfalco, espionaje industrial, sabotaje, errores/omisiones, y falta de disponibilidad de

los sistemas.

La adhesión a estas políticas también ayuda a asegurar que Manpower cumpla con todas las

leyes o regulaciones en América, Europa, Medio Oriente, África, o Asia del Pacífico.

Alcance

Las presentes políticas alcanzan a todos los empleados de Manpower Inc. y a todas sus

entidades comerciales y subsidiarias en todo el mundo. Los empleados temporales,

consultores, y otros usuarios de los recursos tecnológicos y sistemas internos de Manpower

también deberán cumplir con estas políticas (En el presente documento, los términos

“Manpower” y “la empresa” son intercambiables y hacen referencia a todas las entidades

comerciales y subsidiarias de Manpower. De igual modo, el término “empleado” hace

referencia a todos los trabajadores de tiempo completo, medio tiempo, o consultores que

Manpower emplea)

Las entidades comerciales individuales dentro de Manpower pueden implementar o conservar

actuales políticas, estándares o procedimientos relacionados con el uso de los recursos

informáticos por parte de los empleados. Tales políticas, estándares o procedimientos deberán

naturalmente ser utilizados en respaldo de las políticas globales – y salvo justificadas

excepciones no podrán contradecirse con o ser menos restrictivos que las políticas globales.

Todos los empleados deberán conocer y cumplir tanto con las políticas locales como con las

políticas globales.

Política para el uso de recursos informáticos

Introducción

Las solicitudes de excepciones específicas respecto de las políticas globales ya sea por

circunstancias legales, culturales, u otras deben ser enviadas para la consideración del

Gerente Global de Seguridad de la Información conforme a los Lineamientos para las

Excepciones a las Políticas Globales de Seguridad que pueden encontrarse en la página de

Global Information Security en el Global Exchange.

Consecuencias de falta de cumplimiento

En Manpower, creemos que “La Seguridad de la Información nos concierne a todos”. Esto

significa que todos los empleados y usuarios de los recursos informáticos de Manpower

tenemos la obligación de proteger adecuadamente nuestros recursos de información. Todos

debemos conocer, comprender y cumplir con estas políticas. Donde es permitido, y hasta

donde la legislación local lo permite, la empresa se reserva el derecho de monitorear el uso de

los recursos informáticos por parte de los empleados para comprobar el cumplimiento de las

políticas.

La violación o no cumplimiento de alguna de estas políticas puede resultar en acciones

disciplinarias hasta donde la legislación local lo permita – y hasta la desvinculación.

La empresa se reserva el derecho de iniciar acciones legales contra cualquier empleado

(incluyendo empleados temporales, “contratados”, etc.) presentes o pasados, que cause daño

alguno a los activos o reputación de la empresa como consecuencia de ignorar en forma

consciente las presentes políticas.

Comunicaciones de las Políticas

Cada entidad comercial ha nombrado un representante ante el Equipo Global de Seguridad de

la Información (más información sobre los miembros de este equipo se encuentra disponible en

la sección Global Information Security del Global Exchange) Esta persona cumple la función

de “Coordinador local de Seguridad de la Información” para dicha entidad, y es responsable de

la traducción de las políticas al idioma local y su posterior comunicación a todo el plantel.

Todos los empleados deben confirmar que han recibido y comprendido las políticas, así como

también expresar su acuerdo con el compromiso de cumplir con tales políticas. El formato

específico de esta confirmación (física o electrónica) y el proceso para obtenerla queda a

consideración del Coordinador local de Seguridad de la Información. Sin embargo, la

confirmación debe ser obtenida dentro de los primeros 30 días a partir de la fecha ingreso del

empleado al plantel de Manpower. A su vez, todos los empleados deben reconfirmar la

recepción, comprensión y acuerdo de cumplir con las políticas como mínimo en forma anual.

Nombres de Usuario

Política

Cada usuario contará con su propio Nombre de Usuario (ID) para tener acceso a los sistemas

informáticos de Manpower. Los nombres de usuario grupales, genéricos o compartidos no

están permitidos.

Propósito

La intención de esta política es asegurar que todos los usuarios autorizados cuenten con un

identificador único de manera que se puedan manejar y controlar los accesos y procesamientos

adecuados. Esto también permite que se creen huellas apropiadas de auditoria y puedan

llevarse registros de acciones y cambios realizados en el sistema por cada usuario individual.

A su vez, se asegura que cada usuario sea responsable de sus acciones.

Recomendaciones e Información Adicional

No está permitido otorgar nombres de usuario de “invitado” o temporales a los usuarios de los

sistemas. Asimismo, no deben crearse nombres de usuarios grupales o compartidos.

El nombre de usuario (ID) es lo que identifica a cada individuo en los sistemas de Manpower.

Esto significa que cada individuo es responsable de todas las acciones realizadas bajo la

autoridad de su nombre de usuario. La combinación de un ID y una contraseña es lo que da a

los usuarios el acceso a los sistemas de Manpower. Por esta razón, las contraseñas nunca

deben ser reveladas (ver la política “Seguridad de Contraseñas”)

También se recomienda que los nombres de usuario no sean revelados – salvo en los casos en

que personal autorizado de Manpower necesite conocer el ID de un individuo con el objeto de

asistirlo en la resolución de un problema o la realización de otras tareas administrativas.

Seguridad de Contraseñas

Política

Las contraseñas asociadas a los nombres de usuario de los sistemas informáticos deben ser

adecuadamente administradas de manera de preservar su integridad y confidencialidad.

Nunca deben ser compartidas o reveladas en forma alguna a nadie más allá del poseedor

autorizado del nombre de usuario.

Las contraseñas deben ser fáciles de recordar para el dueño legítimo pero a su vez, difíciles de

adivinar para otras personas. Todas las contraseñas deben:

• Tener una longitud de al menos 8 caracteres

• Ser una combinación de caracteres alfanuméricos

• Cambiarse cada 30 días

• Reutilizarse (si lo desea) recién luego de la 13 actualización

Para mayor protección contra posibles ataques, los sistemas deben ser configurados de

manera que las cuentas se inhabiliten luego de 3 intentos fallidos de ingreso. Una vez

inhabilitadas, dichas cuentas no serán reactivadas hasta que el dueño o el jefe inmediato lo

soliciten.

Las solicitudes para reactivar un nombre de usuario o resetear una contraseña no serán

otorgadas hasta tanto el solicitante se identifique adecuadamente como el dueño legítimo del

ID. Si se trata del jefe directo deberá realizar la solicitud mediante un correo electrónico al

departamento de sistemas.

Propósito

Con la intención de ser cordiales, más productivos, o de ganar tiempo, los usuarios a veces

comparten sus contraseñas. Toda vez que los usuarios revelan sus contraseñas, sin quererlo

están comprometiendo los controles de acceso al sistema y haciendo que los registros de

actividad del usuario sean menos útiles. ¡Todos los usuarios deben recordar que son

responsables de todas las acciones realizadas con sus nombres de usuario!

La contraseña es la defensa más importante que Manpower tiene contra usuarios no

autorizados y potenciales intrusos. En última instancia, la contraseña es la barrera entre

información confidencial de un cliente y un usuario no autorizado. Es obligatorio que todas las

contraseñas estén adecuadamente protegidas y administradas.

La intención de esta política es asegurar que las contraseñas sean administradas de manera

tal que sean confidenciales, y no puedan ser adivinadas fácilmente o comprometidas de otro

modo.

Recomendaciones e información adicional

Además de nunca compartir sus contraseñas intencionalmente, los usuarios deben tener

cuidado de no revelarlas accidentalmente. Las contraseñas nunca deben pronunciarse en voz

alta (ya que alguien podría escucharlas) ni deben ser escritas y colocadas en un lugar visible.

En general, las contraseñas nunca deben ser guardadas en forma escrita – en cambio, deben

ser fáciles de recordar para el dueño pero difíciles de adivinar para otros.

Si una contraseña debe ser escrita, se deberán tomar medidas para proteger el papel donde ha

sido escrita. No deje su contraseña escrita en una nota pegada en su computadora o

escondida en un lugar obvio (como debajo del teclado o del Mouse pad) Idealmente, el papel

debería ser guardado fuera del área de trabajo, en un lugar seguro.

Si bien esta política describe los requerimientos mínimos para las contraseñas, todos los

usuarios deben crear contraseñas “robustas” fáciles de recordar pero difíciles de adivinar. A

continuación encontrará algunos consejos útiles para crear una contraseña “robusta”:

1. Combine letras, números, mayúsculas/minúsculas y caracteres especiales.

2. No utilice su nombre, nombre de usuario, u otros valores fáciles de adivinar (como

“contraseña”, "cont", o “default”)

3. No utilice una palabra existente en un diccionario o una secuencia de sólo

números.

4. No utilice secuencias de letras contiguas en el teclado (como ASDFGH) No

obstante, algunos patrones del teclado (como q2w3e4r5t6) podrían ser una

contraseña “robusta” fácil de recordar. De hecho, podría utilizar el mismo patrón al

actualizar su contraseña simplemente cambiando el carácter donde comienza la

secuencia – en vez de comenzar con “q2...”, comience con “w3...” y obtendrá otra

contraseña robusta y fácil de recordar.

5. Piense una frase que recuerde fácilmente y utilice la primera letra de cada palabra

de dicha frase. Reemplace letras o (partes de) palabras por números (“docena” =

“2ena”, o “sin corazón” = “5corazon”, etc.)

La protección adecuada de las contraseñas es la medida de seguridad más efectiva que puede

ser aplicada para proteger apropiadamente los sistemas y la información confidencial que ha

sido confiada a un individuo.

Asignación de niveles de privilegios de acceso

Política

Los niveles de privilegios para que los usuarios accedan a los sistemas informáticos y a los

datos de Manpower serán asignados en base a los requerimientos del puesto de trabajo.

Únicamente deben ser otorgados los permisos mínimos requeridos para que el usuario pueda

desarrollar sus funciones específicas.

Bajo ninguna circunstancia los usuarios obtendrán privilegios de acceso más allá de los

necesarios para realizar sus tareas.

Propósito

La presente política define los niveles de autoridad y acceso que puede otorgarse a un usuario

de los sistemas y datos de Manpower. El objetivo es asegurar que tales privilegios de acceso

sean asignados en función de lo que el usuario “necesita saber”. Es decir, los usuarios

únicamente deben recibir accesos y privilegios pertinentes a su función laboral. Los accesos

adicionales no están permitidos.

Recomendaciones e información adicional

Cuando los usuarios de los sistemas reciben permisos de acceso que exceden sus

necesidades, los mismos tienen la capacidad de realizar acciones que podrían dañar a la

compañía – algunas de las cuales podrían tener consecuencias graves. Tales acciones

pueden realizarse con mala intención pero a veces se trata de accidentes. Al restringir los

privilegios y niveles de acceso a únicamente lo que el empleado requiere para su función, se

minimiza en gran medida el riesgo de que ocurran tales acciones perjudiciales.

Uso de Internet

Política

El acceso a Internet facilitado por Manpower a sus empleados es propiedad de la empresa.

Este acceso debe ser utilizado con el propósito de hacer negocios en nombre de la empresa y

sus clientes.

La utilización de esta herramienta para uso personal no está permitida

La empresa se reservará el derecho de:

•

Bloquear el acceso a cualquier página Web que pueda ser considerada inapropiada o

que pueda significar un riesgo para la integridad de las redes o reputación de la

empresa

Monitorear el uso de Internet por parte del empleado para controlar el cumplimiento de

la presente política

•

Propósito

Esta política define de qué manera los individuos autorizados pueden o no utilizar los recursos

de acceso a Internet provistos por Manpower. El objetivo de esta política es:

•

Proteger las computadoras, las redes y los datos de Manpower de problemas que

podrían surgir de descargar (intencionalmente o no) o ejecutar virus informáticos u

otros tipos de software destructivos de sitios de Internet infectados.

Proteger los servicios de Internet de Manpower para evitar la saturación de la red a

causa de actividades no relacionadas con las actividades de la empresa.

Proteger la reputación de Manpower asegurando que no se obtengan materiales

inapropiados o degradantes utilizando el acceso a Internet provisto por la empresa.

•

•

Recomendaciones e Información Adicional

La utilización de los recursos de Internet de la empresa con propósitos no laborales conlleva

una cantidad de riesgos tales como:

•

Disminución del rendimiento del sistema. Los usuarios legítimos pueden sufrir un bajo

rendimiento o mal tiempo de respuesta a causa de altos volúmenes de actividad que no

sirven a propósitos de la empresa.

Epidemias de virus informáticos. Visitar páginas Web inapropiadas implica un alto

riesgo de infección de virus informáticos u otras clases de software destructivo, dado

que tales sitios generalmente no están administrados con el nivel de seguridad de las

páginas pertenecientes a organizaciones legítimas.

Mayor cantidad de correo electrónico no deseado. Muchos sitios de Internet solicitan al

visitante la dirección de correo electrónico. Estas direcciones pueden ser luego

vendidas a otras firmas de mercadeo que las utilizan para enviar comunicaciones no

solicitadas (conocidas como “spam”) por correo electrónico.

•

•

•

Daños a la reputación de Manpower. Al visitar ciertos sitios, se generan “footprints” o

marcas registrando que el visitante accedió a través de recursos de Internet de

Manpower. Si información de esta clase se conociera públicamente, la reputación de la

Empresa podría verse dañada.

Para evitar estos problemas, los usuarios de Internet de Manpower deben abstenerse de:

•

•

•

•

•

Visitar páginas Web que contengan material pornográfico.

Visitar páginas que promuevan la violencia, la intolerancia, el abuso de drogas/alcohol,

las actividades criminales, o cualquier otro comportamiento objetable o ilegal.

Visitar páginas que promuevan o permitan las apuestas online.

Escuchar la radio o ver televisión por Internet.

Descargar cualquier material que no será utilizado con fines laborales. Esto incluye

(pero no se limita a) material pornográfico, música, y archivos de video.

Comunicaciones Electrónicas

Política

Los sistemas y herramientas de comunicaciones electrónicas (tales como el correo electrónico,

los mensajes instantáneos (chat), el fax, etc.) provistos por Manpower a sus empleados son

propiedad de la empresa. Estos elementos son provistos con el fin de realizar negocios y

tareas laborales en nombre de la empresa y sus clientes.

La utilización de estas herramientas para uso personal no está permitida.

El personal solo puede utilizar estas herramientas para comunicarse con las personas de la

compañía con quienes tiene relación laboral directa.

Toda actividad de negocios realizada a través de una comunicación electrónica debe ser

realizada utilizando únicamente las herramientas provistas por la empresa. Las herramientas o

cuentas personales (incluyendo servicios de terceros como Yahoo, Hotmail, etc.) no están

permitidos para realizar actividades en nombre de la empresa.

La empresa se reserva el derecho de monitorear las comunicaciones electrónicas para

asegurar el cumplimiento de la presente política.

Propósito

Esta política define de qué manera los individuos autorizados pueden utilizar las herramientas

de comunicación electrónica provistas por Manpower. El propósito de esta política es:

•

Evitar la disminución del rendimiento del sistema. Los usuarios legítimos pueden sufrir

un bajo rendimiento o mal tiempo de respuesta a causa de altos volúmenes de

actividad que no sirven a propósitos de la empresa.

Proteger las computadoras, redes y datos de Manpower de problemas que podrían

surgir del uso inapropiado de las herramientas de la empresa.

Proteger los sistemas de Manpower de una potencial sobrecarga de actividad no

relacionada con las tareas laborales.

Proteger la reputación de Manpower asegurando que las herramientas de la compañía

no serán utilizadas para divulgar material inapropiado o degradante.

•

•

•

Recomendaciones e Información Adicional

Se prohíbe el almacenamiento o transmisión de lo siguiente:

•

•

Materiales sexualmente explícitos o sugerentes.

Materiales que promuevan el acoso o menosprecio de otros en función de su sexo,

raza, orientación sexual, edad, nacionalidad, discapacidad o creencias políticas o

religiosas.

Cualquier cosa que sea difamatoria, amenazante, profana, ofensiva, calumniosa, o

invasora de la privacidad de otra persona.

•

Además, a menos que forme parte de un requerimiento laboral definido y aprobado por la

empresa, las siguientes actividades están prohibidas:

•

•

Enviar Spam

Ofrecer servicios no relacionados con la actividad de la Empresa, o con fines

políticos.

Iniciar o continuar “cadenas” de mensajes (cualquier tipo de mensajes con la

instrucción de ser reenviados – incluyendo alertas de virus)

Enviar mensajes con archivos ejecutables adjuntos.

Enviar información que pueda ser confidencial o tener derechos reservados.

•

•

•

Uso de la Red, Software y Datos

Política

Las redes informáticas, el software y los datos son provistos por Manpower a los usuarios

autorizados con el único propósito de realizar negocios en nombre de la empresa y sus socios

comerciales. Se prohíbe el uso de las redes informáticas, el software o los datos con otros

fines.

Propósito

Esta política define de qué manera los individuos autorizados pueden o no utilizar los recursos

de redes, software y datos de Manpower. Se busca proteger estos activos de:

1. Daños por parte de usuarios no autorizados o divulgación de información a usuarios no

autorizados.

2. Saturación de los recursos por excesos de actividad no relacionada con actividades

laborales.

Recomendaciones e Información Adicional

Esta política prohíbe que los individuos no autorizados utilicen los recursos de la red

informática, software y datos provistos por Manpower. El uso por parte de cualquier individuo

no autorizado representa una clara violación de esta política.

Asimismo, los recursos de red informática, el software y los datos provistos por Manpower no

pueden ser utilizados para hacer negocios para otras empresas o individuos, ni deben ser

utilizados con fines personales. En especial, los recursos de almacenamiento en red de la

empresa no pueden ser utilizados para almacenar datos personales como fotos, música, videos

u otros contenidos que no estén directamente relacionados con las actividades laborales dentro

de la Manpower y/o sus empresas afiliadas y socios comerciales.

Protección de Equipos portátiles

Política

Todos los dispositivos informáticos portátiles (como laptop, notebook, o computadoras de

mano) deben ser físicamente protegidos de pérdida o robo. Específicamente, los usuarios

deben asegurarse de que sus equipos informáticos estén físicamente asegurados cuando no

los tienen con ellos. Esto puede hacerse utilizando estaciones de seguridad (locking docking

station), un cable de seguridad debidamente asegurado, o bien, guardar los dispositivos en un

armariobajollave.

Los usuarios nunca deben dejar equipos portátiles desatendidos en lugares públicos.

Es obligación informar inmediatamente cualquier incidente de robo o pérdida de un equipo de

la empresa.

Propósito

El propósito de esta política es asegurar que los dispositivos de hardware y los datos sean

adecuadamente protegidos de daño, robo o uso indebido.

Recomendaciones e Información Adicional

Todos los empleados que utilicen equipos portátiles deben seguir los siguientes lineamientos:

•

Nunca deje su equipo portátil desatendido en su oficina o en la oficina de un cliente u

otro lugar a menos que esté correctamente asegurada con un cable de seguridad u

otro mecanismo.

Si utiliza un cable de seguridad, asegúrese de que el mismo esté unido a un objeto fijo,

que no sea fácil de mover, levantar o de hurtar junto con la computadora.

•

Si viaja:

•

Lleve su laptop en un estuche reforzado, que proteja el equipo de golpes. Es

aconsejable utilizar un estuche que no sea propiamente para transportar laptops para

que el contenido no sea tan evidente. Colocar el estuche en un bolso más grande, por

ejemplo una mochila deportiva es una buena forma de “disfrazar” su computadora.

Nunca despache, documente o facture su computadora con el resto del equipaje.

Llévela siempre con su equipaje de mano. El riesgo de robo o daño es mayor que

cualquier beneficio.

Preste especial atención cuando espera haciendo fila en los puntos de seguridad de los

aeropuertos, ya que podría suceder que un delincuente genere una distracción y su

cómplice robe su laptop. Observe cuidadosamente cuando su laptop está pasando por

la cinta de rayos.

Nunca deje su equipo portátil desatendido en lugares públicos (como restaurantes,

lobbies de hotel, áreas de espera de los aeropuertos, etc.)

Si debe dejar su laptop en un automóvil, asegúrese de que el vehículo quede cerrado y

que la laptop no quede a la vista. Idealmente, debería estar en el baúl/cajuela.

Utilice su cable de seguridad si debe dejar su laptop desatendida en un cuarto de hotel.

Asegúrese de que está correctamente conectado a un objeto que sea difícil mover.

•

•

•

•

•

Otra alternativa sería dejar la computadora en la caja de seguridad (si el tamaño lo

permite) o en un cajón con llave.

Protección de sistemas inactivos o desatendidos

Política

Todos los usuarios deben cerrar la sesión (log off) de sistemas o aplicaciones que no utilizarán

por un período de tiempo. Como mínimo los usuarios deben salir de los sistemas al final de

cada jornada laboral.

Al dejar una estación de trabajo desatendida, el usuario debe bloquear el equipo utilizando una

contraseña en el protector de pantalla u otro método para evitar que usuarios no autorizados

tengan acceso a cualquiera de los sistemas activos en ese equipo.

Propósito

Esta política tiene como objeto asegurar que usuarios no autorizados no tengan acceso

fácilmente a la computadora de un usuario legítimo – accediendo así a información confidencial

o de privilegio. La adhesión a esta política ayudará a asegurar que los datos y los sistemas

estén adecuadamente protegidos de daño, robo o uso indebido.

Recomendaciones e información adicional

Siga las instrucciones estándar de cerrar sesión de cada sistema que utiliza.

El sistema se configurará desde el departamento de informática para que transcurridos 5

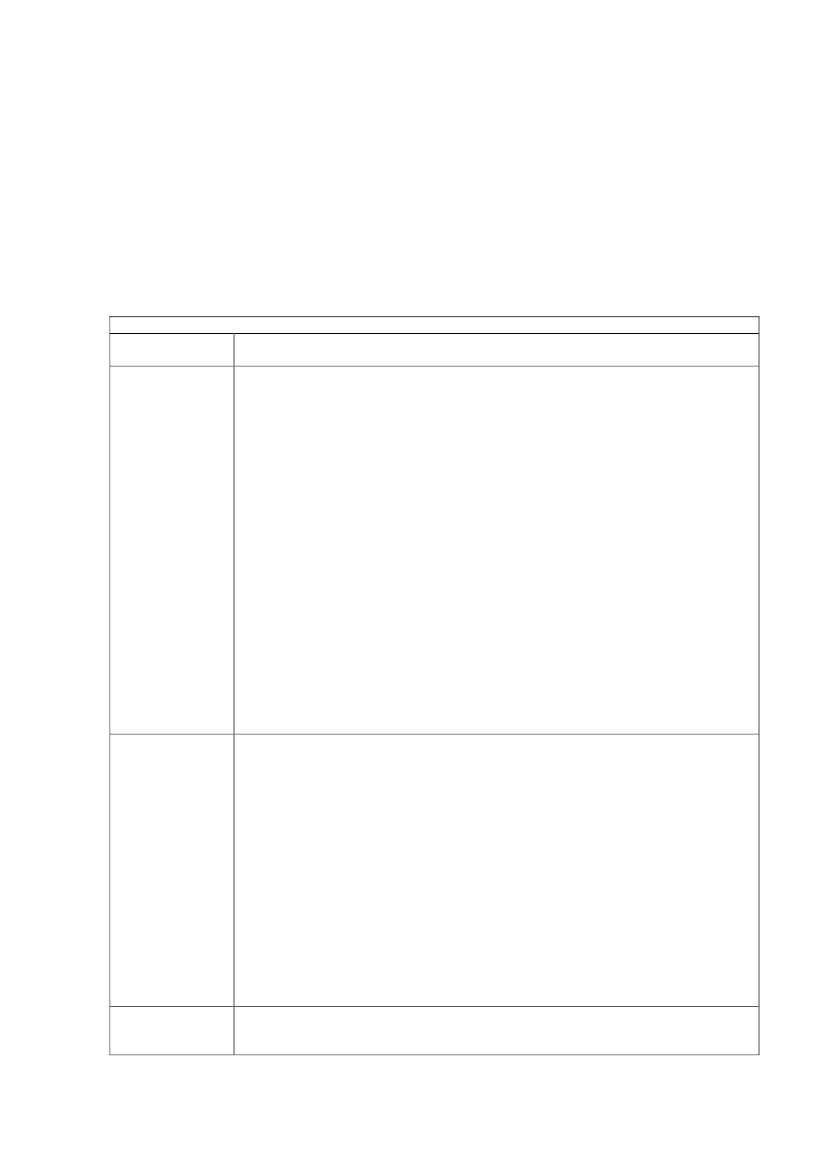
minutos sin actividad, la computadora bloquee la sesión de trabajo, siendo necesario el ingreso

de la contraseña de red para normalizar la sesión. Esta configuración no podrá ser aumentada

por el usuario debido a que compromete la seguridad de las aplicaciones de la compañía.

En la documentación de cada sistema para el usuario se deberán especificar las

particularidades en relación al cierre de sesión.

Protección de la información

Política

Toda información en poder de Manpower debe ser protegida de acuerdo con la categoría de

“Protección de Datos” a la que pertenezca. Estas medidas de seguridad deben ser aplicadas a

todos los datos – incluyendo tanto datos en uso como datos guardados en unidades de

respaldo (backups)

Para cada categoría definida, los niveles mínimos exigidos de protección que deben ser

implementados son los siguientes:

Categorías de protección de datos y medidas de protección

Categoría de la Medidas de protección mínimas

información

ConfidencialEl acceso está restringido sólo a aquellos individuos que “necesitan conocer la

(Alta)información”. Este acceso es otorgado sólo a un número limitado de individuos.

Los papeles o medios extraíbles tales como discos compactos, diskettes, cintas,

memorias flash, etc. que contengan información confidencial no deben ser

dejados al alcance de cualquiera. Tales papeles y dispositivos deben ser

guardados en áreas seguras (como por ejemplo un cajón o armario con llave)

mientras no están en uso o no son vigilados.

Toda información confidencial guardada en un dispositivo portátil (como una

laptop, PDA, “Blackberry”, etc.) o en medios extraíbles (discos compactos,

diskettes, cintas, memorias flash, etc.) debe estar encriptada.

Está prohibido dar a conocer información confidencial fuera de la empresa, a

menos que Notificaciones de Privacidad correspondientes, permisos de los

individuos, políticas, procedimientos, lineamientos o contratos con clientes o

socios comerciales lo permitan. En todos los casos, la divulgación de información

confidencial únicamente está permitida cuando quien la recibe, “necesita

conocerla” para cumplir con su trabajo.

Cuando ya no se los necesitará, todos los medios que contengan datos

confidenciales deben ser destruidos o debidamente desechados de forma segura

y en cumplimiento con todas las políticas aplicables a la retención de documentos.

El acceso está restringido sólo a aquellos individuos que “necesitan conocer la

información”.

Los papeles o medios extraíbles tales como discos compactos, diskettes, cintas,

memorias flash, etc. que contengan información restringida no deben ser dejados

al alcance de cualquiera. Tales papeles y dispositivos deben ser guardados en

áreas seguras mientras no están en uso o no son vigilados.

La divulgación de información restringida únicamente está permitida cuando quien

la recibe, “necesita conocerla” para cumplir con su trabajo y debe hacerse de

acuerdo con todas las políticas aplicables, procedimientos, lineamientos o

contratos o clientes y socios comerciales.

Cuando ya no se los necesitará, todos los medios que contengan datos

confidenciales deben ser destruidos o debidamente desechados de forma segura

y en cumplimiento con todas las políticas aplicables a la retención de documentos.

Interna

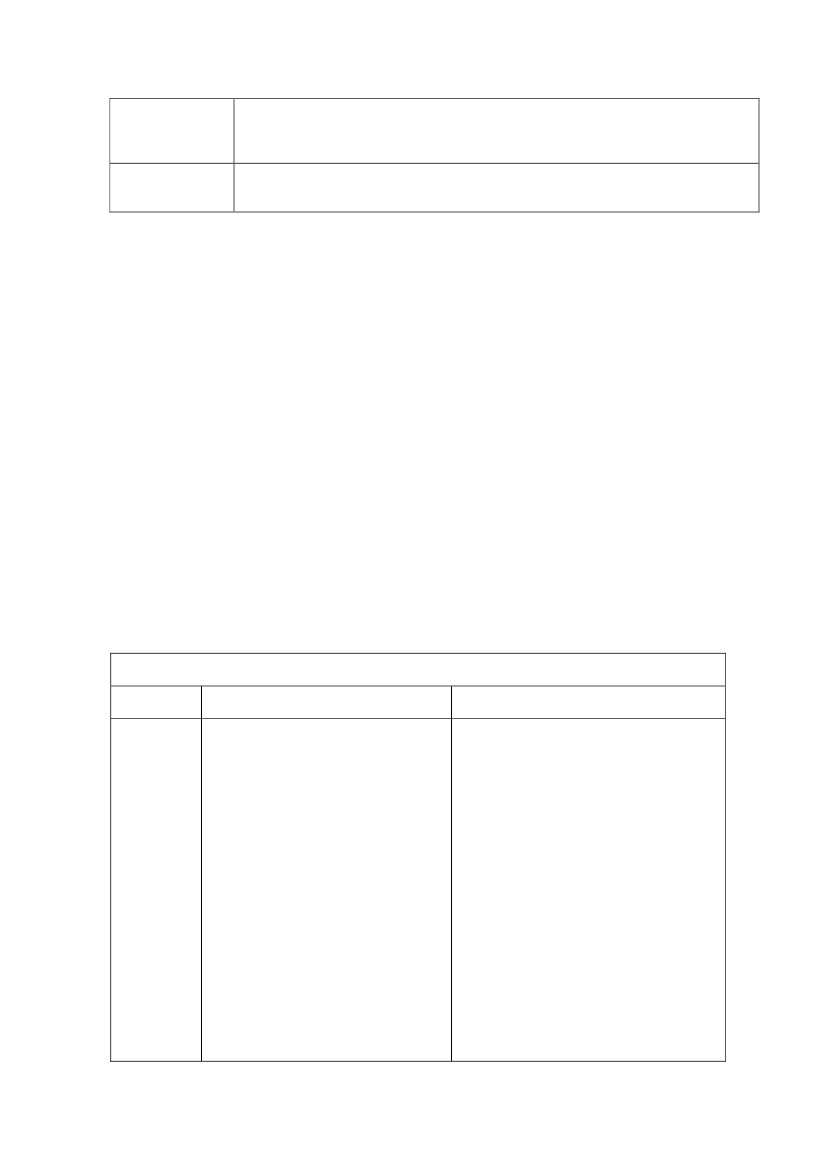
(Media)

No se exigen precauciones especiales si la información es manejada dentro de la

empresa.

Restringida

(Media-alta)

Pública

(Baja)

Los datos pueden ser dados a conocer fuera de la empresa siempre y cuando

existan razones comerciales legítimas.No obstante, deberán tomarse

precauciones razonables para evitar que la información llegue a individuos no

autorizados fuera de la empresa.

No se requieren precauciones especiales.

Puede ser distribuida libremente fuera de la empresa.

Propósito

La presente política ayuda a asegurar que los activos de información de Manpower estén

guardados en forma segura y apropiada durante su ciclo completo en poder de Manpower. Los

usuarios autorizados de la información son los responsables de aplicar todas las medidas de

seguridad requeridas para proteger los datos adecuadamente contra daños, alteración o

divulgación inapropiada.

El cumplimiento de esta política ayudará a proteger la información de la empresa –

especialmente la información confidencial y restringida – de robo o pérdida. Esto nos ayudará

a proteger la privacidad de nuestros empleados permanentes, temporales, clientes,

proveedores y contratistas lo cual a su vez, ayudará a proteger la marca Manpower y la

reputación de la empresa.

Asimismo, la empresa puede tener obligaciones contractuales con clientes para mantener tal

información almacenada en forma segura. En caso de dudas, deberá contactarse un asesor

legal para determinar el tipo de información a ser protegida en cumplimiento con esta política.

Recomendaciones e información adicional

Las definiciones de las categorías de protección de datos enumeradas abajo ofrecen un vistazo

general sobre las diferencias entre las diversas categorías mencionadas en esta política y

aportan una lista de datos representativos que deben ser considerados para su protección

dentro de su respectiva categoría.

Categorías de protección de datos, definición y datos a ser considerados para su

protección

CategoríaDefiniciónDatos a ser considerados para su

protección

Confiden-

cial (Alta)

Información que sólo está disponible

para un grupo muy limitado de

individuos dentro del grupo de

empresas de Manpower, o bien,

clientes,proveedoreso

subcontratistas autorizados.El

acceso es otorgado únicamente si el

individuo “necesita conocer” la

información.

La divulgación no autorizada de estos

datos probablemente resulte en un

impacto significativamente adverso,

conflictos, o castigos a la empresa.

La divulgación puede causar un alto

riesgo de robo de identidad,

exposición de información con

derechosreservadosoviolar

legislaciónrelacionadaconla

protección de datos.

Datos sensibles de un individuo tales

como:

• Número de seguridad social, número

del seguro social, DNI, CURP,

pasaporte,cédula nacional de

identidad, o identificación nacional de

identidad

• Información médica incluyendo la

capacidad para trabajar y ausencias

por enfermedad

• Número de licencia de conducir

• Fecha de nacimiento

• Números de tarjetas de crédito o

cuentas bancarias

• Averiguacióndeantecedentes

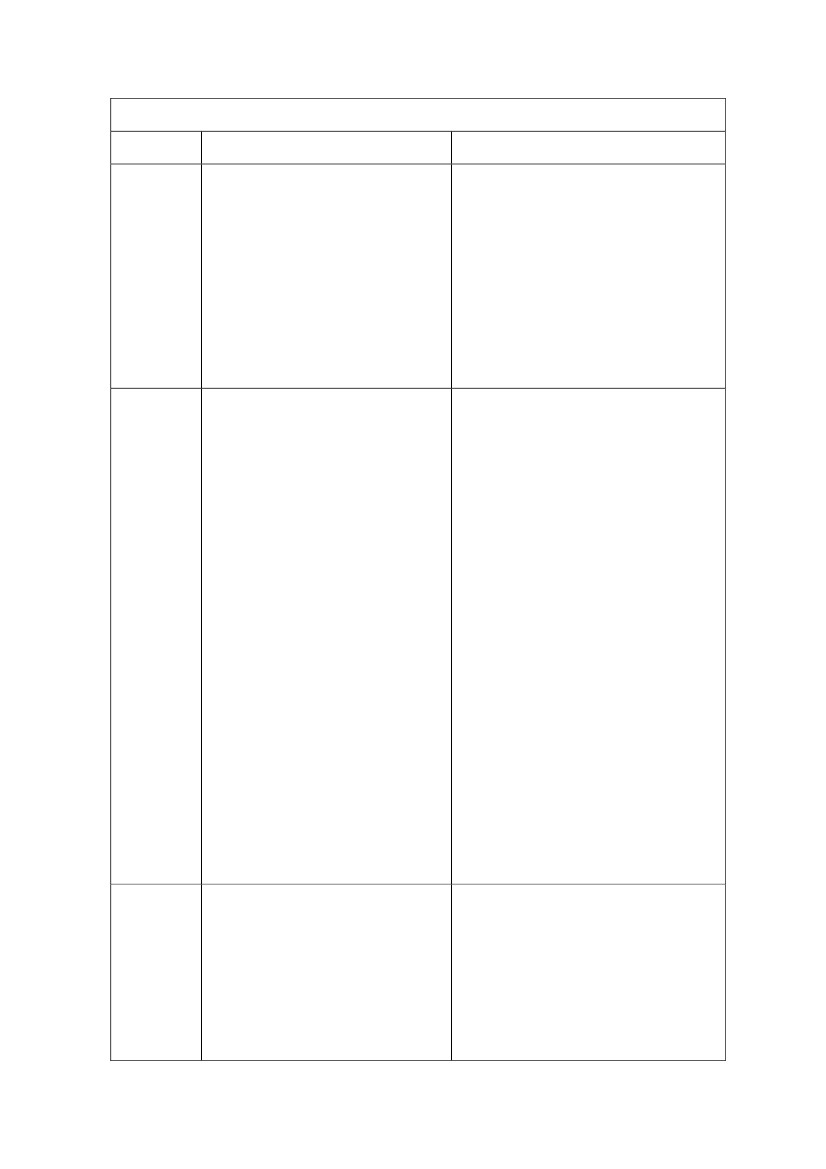
policiales o criminales/penales.

• Raza, origen étnico, opiniones

políticas, creencias religiosas o

filosóficas, afiliación a sindicatos o

uniones de trabajadores, o vida u

Categorías de protección de datos, definición y datos a ser considerados para su

protección

CategoríaDefiniciónDatos a ser considerados para su

protección

orientación sexual

Los registros del personal incluyendo

evaluaciones de desempeño, información

del salario, beneficios y compensaciones,

y asuntos legales.

Información relacionada con controles de

seguridadinternatalescomo

configuración del firewall u otras

configuraciones.

Restringida

(Media-alta)

Información que sólo está disponible

para un grupo específico de

individuos dentro del grupo de

empresas de Manpower, o bien,

clientes,proveedoreso

subcontratistas autorizados.

El acceso es otorgado únicamente si

el individuo “necesita conocer” la

información.

La divulgación no autorizada de estos

datos puede resultar en un impacto

moderadamente adverso, conflictos,

o castigos a la empresa.La

divulgación puede violar legislación

relacionada con la protección de

datos.

Información personal perteneciente a

candidatos, empleados permanentes y

temporales tal como: información de

contacto (incluyendo nombres, domicilio

postal, dirección de correo electrónico,

númerostelefónicos),educación,

conocimientos y aptitudes, referencias,

experiencialaboral,preferencias

laborales,expectativassalariales,

curricula vitae, pruebas de evaluación del

candidato, etc.

Datos personales pertenecientes a

individuos empleados por clientes,

proveedores o subcontratistas tales como

información de contacto, números de

control impositivo, facturación o datos de

facturas, etc.

Información relacionada con productos,

prototipos, procesos, información de

ventas mercadeo, información técnica,

secretosdetransacciones,ideas,

inventos, experiencia, know-how, datos

de clientes, información financiera, listas

de precios , tarifas de pago, descuentos,

propuestascomercialesytoda

información contenida en libros y

registros corporativos.

Interna

(Media)

Información que está disponible para

todos los empleados de Manpower

pero generalmente no para individuos

externos.

Destinada a su uso dentro de la

empresa.

La divulgación no autorizada no

causaríaunimpactoadverso

Publicaciones de noticias de la empresa

o departamentales, documentos sobre

políticas y procedimientos generales.

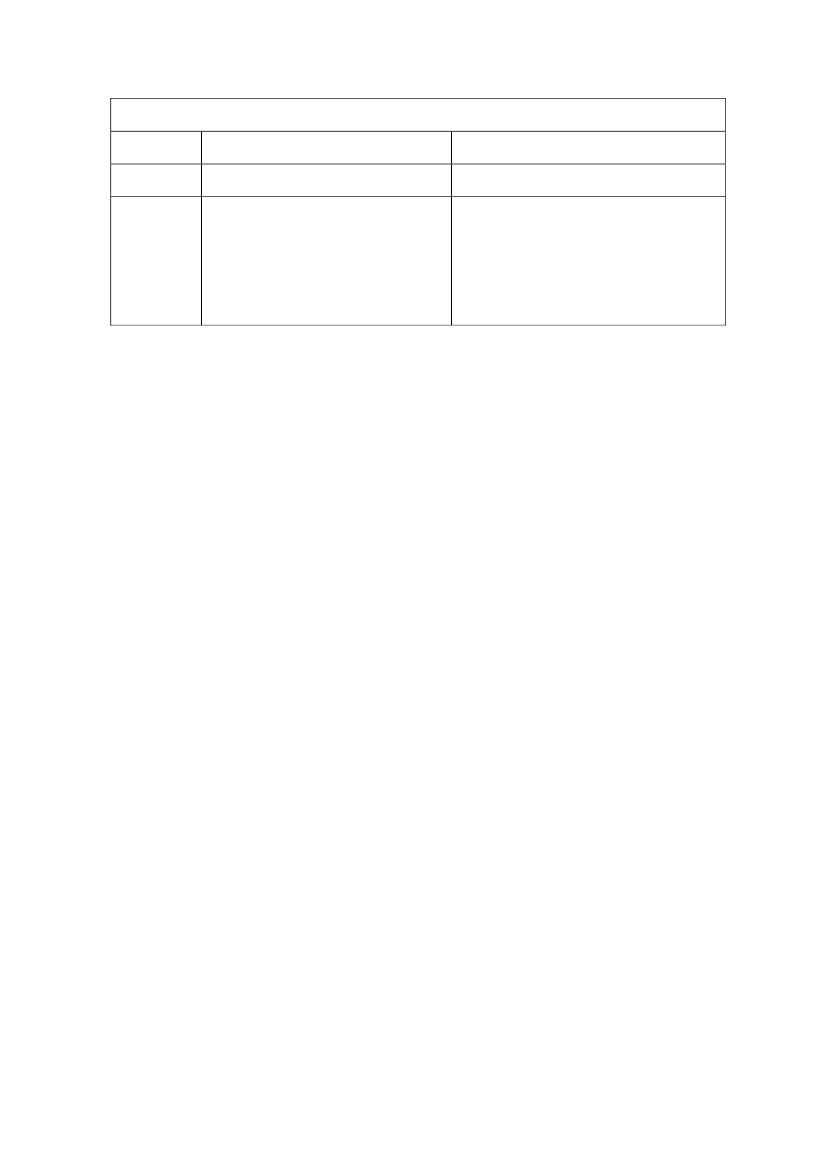
Directorios telefónicos

nombreynúmeros

comerciales y ubicación.

locales con

deteléfono

Categorías de protección de datos, definición y datos a ser considerados para su

protección

CategoríaDefiniciónDatos a ser considerados para su

protección

significativo.

Pública

(Baja)

Información generalmente disponible

sin restricciones para el público en

general.

La divulgación de esta información no

tendría un impacto negativo en la

empresa.

Direcciones y números telefónicos de las

oficinas,materialespúblicosde

mercadeo, publicaciones de noticias,

folletos de publicidad, clasificaciones e

informes anuales.

Es importante recordar que todos los medios conteniendo información confidencial o restringida

deben ser adecuadamente destruidos antes de ser desechados. Todos los documentos en

papel deben ser triturados antes de ser desechados. Ciertos medios magnéticos como

diskettes, cintas, discos compactos, etc. también pueden ser destruidos dependiendo de las

características de la máquina disponible a tales fines. Si estos medios no pueden destruirse

utilizando la máquina trituradora, deberán aplicarse otras técnicas manuales de destrucción

física de los elementos.

Protección contra Virus

Política

Los usuarios no deben introducir en las computadoras código diseñado para afectar el

rendimiento de o acceso a cualesquiera de los sistemas redes, o datos de Manpower. (Por ej.

Virus informáticos, worms, troyanos y otras clases de software maligno)

Todas las estaciones de trabajo están equipadas con software antivirus actualizado. Para

asegurar su efectividad, los usuarios deben:

•

•

Mantener el software activo siempre.

Utilizar el software para confirmar la presencia de un virus cuando existen sospechas

del mismo.

Informar cualquier problema encontrado al intentar detectar o erradicar un virus.

Cumplir inmediatamente con todas las directivas dadas a conocer por el personal de

soporte sobre las formas de reparar daños, o mitigar el riesgo en una computadora

infectada.

Nunca instalar otro software antivirus.

•

•

•

Los usuarios NO deben enviar advertencias de virus o software maligno a otros individuos

especialmente mediante el sistema de correo electrónico de Manpower.

Propósito

La presente política ha sido definida con el objeto de asegurar que existan las prácticas

técnicas y administrativas apropiadas para identificar y eliminar infecciones de virus de los

sistemas informáticos de Manpower.

Recomendaciones e información adicional

Todos los sistemas informáticos de Manpower están protegidos de virus, Works, troyanos y

otros tipos de software maligno (conocidos también como “malware”) Esta protección incluye el

uso de software antivirus especializado que escanea los archivos en busca de la presencia de

tal malware. El software ha demostrado ser muy efectivo para detectar y detener infecciones

de virus, pero ningún antivirus puede ser considerado “infalible”. Por tal razón, todos los

usuarios deben tomar precauciones adicionales para ayudar a proteger los equipos de

infecciones de virus:

•

Sospeche de mensajes de correo electrónico o archivos adjuntos inesperados – aún

cuando el mensaje llega de alguien a quien usted conoce y en quien confía. El correo

electrónico y los archivos adjuntos son actualmente el mecanismo más común de

distribución de virus y el mensaje que los contiene es usualmente generado

automáticamente sin que el remitente sepa lo que está sucediendo.

Sea cauteloso si debe descargar un archivo de Internet. Las empresas más

respetables cuentan con medidas antivirus en sus páginas web, pero muy pocas de

ellas garantizan que el software que se descarga de sus sitios no contiene virus.

•

La instalación de software antivirus no provisto o aprobado por Manpower puede causar otros

problemas al usuario – incluyendo incompatibilidades en el sistema, degradación del

rendimiento y fallas inesperadas del equipo. Por esta razón, los usuarios NO deben intentar

instalar ningún tipo de software antivirus adicional.

Se recomienda que los usuarios sean escépticos de cualquier mensaje de correo electrónico u

otro anuncio que reciban advirtiendo sobre un nuevo virus y sus consecuencias si el equipo es

infectado. La mayoría de tales mensajes tienen por objetivo generar miedo. Generalmente,

solicitan al receptor que reenvíe el mensaje a todos sus contactos – inundando de esta forma

los sistemas de correo con advertencias y saturando los servidores de correo al punto que

podrían presentar fallas. En caso de recibir este tipo de advertencias, el usuario puede

reenviarla al responsable de seguridad de sistemas de Manpower para su verificación. No

obstante, en la mayoría de los casos, estas advertencias son falsas y pueden ser ignoradas.

Bajo ninguna circunstancia estas advertencias deben ser enviadas a otros usuarios.

Implementación de ajustes de seguridad

Política

Todos los ajustes, parches y medidas de mantenimiento de software provistos por el personal

de soporte técnico de Manpower deben ser aplicados en tiempo y forma. Aquellas

actualizaciones consideradas críticas deben ser "forzadas" directa e inmediatamente en cada

computadora en cuanto se conecta a la red.

Los usuarios NO deben intentar aplicar ninguna actualización o parche a ningún software a

menos que la actualización sea indicada directamente por el personal de soporte técnico de

Manpower.

Propósito

Esta política tiene dos objetivos principales:

•

•

Asegurar que las actualizaciones y parches de sistemas sean aplicados en tiempo y

forma.

Evitar que se apliquen prematuramente parches no probados en las computadoras

conectadas a la red de Manpower.

Para proteger adecuadamente los equipos de ataques de virus, worms, y otros tipos de

software maligno, es esencial que las computadoras se mantengan actualizadas con las

últimas versiones de antivirus. No obstante, también es esencial que tales actualizaciones no

sean aplicadas hasta que hayan sido probadas y verificadas adecuadamente por el personal de

soporte técnico correspondiente.

El cumplimiento de esta política ayuda a proteger las computadoras de Manpower de

potenciales infecciones, riesgos o daños a causa de software maligno o la prematura aplicación

de actualizaciones en los sistemas.

Recomendaciones e información adicional

Manpower emplea muchos especialistas en tecnología cuya labor es monitorear y defender la

red y todas las computadoras conectadas a la misma. Estos individuos están siempre al tanto

de los últimos desarrollos y amenazas que pudieren surgir – incluyendo la propagación de virus

informáticos, troyanos y otros tipos de software maligno. Tan pronto como salen nuevos

parches, actualizaciones u otras medidas de protección, estos especialistas deben probarlas y

verificar su compatibilidad con el software existente. Debe determinarse la gravedad de cada

amenaza individualmente y tomar la decisión apropiada sobre cómo distribuir el parche o

actualización correspondiente. En general, los parches y actualizaciones considerados

“críticos” deben instalarse lo más rápido posible. Otros, menos críticos, pueden incluirse en el

ciclo de actualización del mantenimiento del software.

La implementación exitosa de cualquier medida de protección depende de las medidas que

tome el usuario de cada computadora. Cuanto antes se apliquen estas medidas de seguridad,

existirán menos probabilidades de que una computadora se vea dañada, corrompida o

comprometida. Bajo ninguna circunstancia los usuarios pueden descargar actualizaciones o

parches de ninguna fuente que no sea la red de Manpower. Los usuarios pueden estar

seguros de que los parches provistos por la empresa han sido sometidos a pruebas de

compatibilidad con el software existente.

Informe de cambios en el personal

Política

Los cambios en la función, responsabilidad o estado de un usuario deben ser informados

inmediatamente a las personas responsables del mantenimiento de los privilegios de acceso de

los usuarios a los sistemas. Ante un cambio, los privilegios de acceso del usuario deben ser

actualizados según las necesidades del caso.

Todos los casos de desvinculación laboral deben ser notificados de inmediato para que los

privilegios de acceso del individuo sean revocados con celeridad.

Propósito

El objetivo de la presente política es ayudar a asegurar que los niveles de acceso de los

usuarios sean siempre acordes con sus funciones; a su vez, que el acceso de los empleados

desvinculados a la red de Manpower sea interrumpido inmediatamente. Ningún usuario debe

tener privilegios de acceso a un sistema que no utilice para realizar sus funciones.

Recomendaciones e información adicional

El personal administrativo correspondiente debe ser informado de los cambios que se

produzcan en el personal para que puedan hacer los ajustes necesarios rápidamente. Deberá

notificarse de inmediato cada vez que un empleado es contratado, transferido o desvinculado,

así como cada vez que se asignan o revocan responsabilidades significativas a un usuario. La

responsabilidad de notificar el cambio recae en la persona responsable de contratar, promover

o desvincular el usuario en cuestión.

Los administradores son responsables de asegurar que los privilegios de acceso que otorgan

sean los adecuados para la función del individuo. No deben otorgarse privilegios o niveles de

acceso más allá de lo estrictamente necesario según las tareas del usuario. Cuando un

usuario recibe niveles de acceso superiores a los que necesita, podría llevar a cabo acciones

perjudiciales para la empresa – algunas de las cuales podrían tener consecuencias graves.

Tales acciones pueden ser malintencionadas pero también pueden ser accidentales. Al

restringir privilegios y niveles de acceso a sólo aquello que el usuario necesita para realizar sus

funciones, la probabilidad de tales acciones dañinas se reduce notablemente.

Informe de incidentes de seguridad

Política

Todos los incidentes de seguridad de la información o violaciones de las políticas de seguridad

deben ser informados de inmediato. Los incidentes o conductas dudosas también deben ser

informados.

Los empleados deben informar estos incidentes directamente a su mesa de ayuda local,

responsable de seguridad informática, responsable de protección de datos, o a su supervisor

directo.

Propósito

El objetivo de esta política es minimizar pérdidas y exposición de la empresa a causa de

incidentes de seguridad de la información. Al confeccionar informes de incidentes reales o de

los cuales se sospecha, puede detectarse un patrón de conducta más amplio que podría

indicar actividad maliciosa. Las demoras en informar tales incidentes podrían resultar en

pérdidas adicionales para la Empresa.

Recomendaciones e información adicional

Los incidentes de seguridad informática que deben ser informados de inmediato incluyen

violaciones a las políticas de seguridad informática vigentes y cualquier caso de pérdida o robo

de equipos. Otras actividades o incidentes que parezcan sospechosos o cuestionables

también deben ser informados.

Merece especial atención la sospecha del uso de “ingeniería social” intentando aplicar trucos

psicológicos con el objeto de obtener información para tener acceso a un sistema informático.

Por lo general, la ingeniería social es perpetrada por teléfono, pero el uso de otros métodos

como el correo electrónico y las páginas Web maliciosas va en aumento. Quien llama puede

identificarse como miembro del equipo de mesa de ayuda, o como asistente de un ejecutivo de

alto rango, y solicitar información (posiblemente incluyendo nombres de usuario y contraseñas),

que luego utilizará para atacar o comprometer sistemas informáticos de la empresa.

Nunca debe proveerse información sobre otros empleados o detalles sobre redes de sistemas

internos o aplicaciones a menos que la identidad del solicitante sea debidamente verificada, y

se haya determinado que el solicitante tiene una necesidad válida y está autorizado a recibir la

información. El potencial uso de una técnica de ingeniería social es considerado una conducta

sospechosa, y debe ser informado inmediatamente.

Uso del Módem

Política

Los módems de las computadoras conectadas a las redes de Manpower deben estar

configurados para acceso “llamadas salientes” únicamente. Bajo ninguna circunstancia estos

módems pueden permitir llamadas entrantes.

Propósito

Los módems son utilizados para conectar computadoras y redes remotas a través de líneas

telefónicas. Esta política tiene por objetivo evitar que los usuarios permitan que se pueda

acceder a sus computadoras en forma remota. Esto disminuye el riesgo de que usuarios no

autorizados tengan acceso a computadoras con información confidencial. También reduce el

riesgo de que se pueda acceder a la red de Manpower a través de una computadora

vulnerada.

Recomendaciones e información adicional

Las computadoras conectadas a líneas públicas de teléfono a través de módems han

demostrado ser extremadamente vulnerables ante ataques externos. Existen técnicas como

“war dialing” las cuales son empleadas para detectar computadoras conectadas y ejecutarles

“exploits” comunes(técnicas que aprovechan vulnerabilidades o errores de programación)

La protección más efectiva ante tales ataques es desconectar completamente la línea de

teléfono de las computadoras equipadas con módem. En muchos casos, sin embargo, esta

medida es impráctica ya que la conexión vía módem es necesaria para permitir que la estación

de trabajo se conecte a una computadora o red remota. En tales casos, el módem deberá

estar configurado para permitir únicamente llamadas salientes. Es decir, que la función de

“auto-respuesta" debe estar deshabilitada para que no se reciban llamadas entrantes. De esta

forma se evita que atacantes externos se conecten o tomen control de la computadora.

Acceso remoto

Política

El acceso a las redes de Manpower (y a cualquier computadora conectada a ellas) desde sitios

remotos está permitido únicamente utilizando las herramientas provistas por la Empresa.

Propósito

El propósito de la presente política es proteger los sistemas y redes de Manpower de daños o

riesgos a los que podrían verse expuestos como resultado del uso de herramientas de acceso

remoto no autorizadas. La intención es ayudar a proteger las computadoras utilizadas por los

empleados de Manpower de daños causados a raíz del uso de tales herramientas.

Recomendaciones e información adicional

Existe una variedad de herramientas y servicios que ofrecen la capacidad de acceder a o

controlar remotamente otras computadoras conectadas a Internet. Si bien muchas de estas

herramientas incluyen algunos mecanismos básicos de seguridad destinados a brindar

protección ante el uso no autorizado, su utilización implica un riesgo significativo para la

seguridad de los equipos expuestos a estos, y para cualquier red a la que las computadoras

expuestas están conectadas. Estos riesgos incluyen:

• La capacidad de propagar virus informáticos y otro software maligno con mayor

facilidad.

• La capacidad de interceptar contraseñas y otros datos confidenciales que

viajen a través de conexiones a Internet no seguras.

• La captura de contraseñas y otros datos confidenciales a través del uso de

software “keystroke logging” - esta tecnología es principalmente usada para

diagnosticar errores en la programación que puede estar instalado en

computadoras de uso público o en “Cyber Cafés”, locutorios, etc.

El uso de software de control remoto para acceder a computadoras en forma remota en una

oficina de Manpower puede ser especialmente peligroso, dado que las computadoras dentro de

las oficinas pueden estar conectadas directamente a la red (WAN) de Manpower. Esto significa

que una computadora vulnerada, en una oficina de Manpower podría ser utilizada para

comprometer las redes internas y datos de la Empresa.

Por tales razones, el uso de software de control remoto no provisto específicamente y

autorizado por Manpower está prohibido.

Hardware de red no autorizado

Política

El hardware de red (routers, switches, servidores, etc.) instalado en cualquier oficina de

Manpower o directamente en cualquier red informática de Manpower debe tener ciertas

características y configuración aprobadas por personal autorizado de Manpower. Dicho

hardware sólo puede ser instalado por aquellos individuos que han sido expresamente

autorizados por Manpower para realizar tal tarea.

La empresa se reserva el derecho de deshabilitar o quitar cualquier hardware que no cumpla

con lo expresado en esta política.

Propósito

Esta política tiene como objeto proteger las redes y datos de Manpower ante daños y riesgos a

causa de dispositivos de red mal configurados o administrados. Cuando dispositivos no

autorizados o mal configurados son conectados a la red, pueden introducirse problemas en la

seguridad y vulnerabilidad, incluyendo:

1. Incapacidad de instalar parches de seguridad y actualizaciones.

2. Problemas para instalar actualizaciones de antivirus en tiempo y forma.

3. Riesgo para las redes y datos de la empresa ante el acceso de usuarios externos no

autorizados.

4. Informes de inventarios deficientes o incompletos.

Recomendaciones e información adicional

Si se determina que una oficina necesita hardware de red adicional, la compra, configuración e

instalación de tal dispositivo deberá coordinarse con el personal autorizado para desempeñar

tales funciones. De esta forma se asegura que el hardware es instalado y configurado

contando con los mismos niveles de protección que el resto de la red. También ayudará a

mantener otros equipos dentro de la oficina protegidos contra una variedad de potenciales

debilidades:

1. Si los parches de seguridad no pueden ser implementados adecuadamente a causa de

la presencia de un dispositivo no autorizado, otras estaciones de trabajo y hardware de

la red conectados a tal dispositivo pueden también verse afectados.

2. A menos que el hardware de red de una oficina esté instalado y configurado

correctamente, las actualizaciones de antivirus no podrán ser distribuidas. Esto podría

resultar en mayores probabilidades de infección de virus informáticos y otros

programas de software maligno.

3. Los routers y redes de área local (LAN) inalámbricas mal instalados o configurados son

particularmente propensos a ser vulnerados por individuos externos. Tal ataque podría

llevar a severa degradación del funcionamiento de la red a causa del aumento de

tráfico procedente de fuentes externas no autorizadas.

4. Los dispositivos mal configurados podrían causar que los inventarios automáticos de

software, estaciones de trabajo, servidores y otros dispositivos se generen con errores.

A su vez, esto podría conducir a una incapacidad para reconocer y reaccionar ante

amenazas de seguridad y ataques que podrían pasar sin ser detectados. También, la

empresa podría encontrarse en violación de acuerdos de licenciamiento de software

ante los proveedores de software.

Software no autorizado

Política

En las computadoras pertenecientes a la empresa se podrá instalar únicamente software

autorizado y licenciado por Manpower. Los usuarios no deben instalar ningún otro software en

las computadoras pertenecientes a Manpower.

La compañía utiliza medios electrónicos para realizar un inventario de todos los programas de

software instalados en cada computadora conectada a las redes de Manpower.

Propósito

Esta política tiene por objetivo proteger las computadoras de daños a causa de la instalación o

uso de software no autorizado. Se busca también proteger los sistemas y redes de Manpower

contra daños que pudieren ocurrir a causa de la instalación de software maligno instalado en

computadoras que se conectan regularmente a las redes de la empresa.

Recomendaciones e información adicional

Se prohíbe a los usuarios instalar programas de software no autorizados específicamente por

la empresa. Manpower provee todos los programas de software necesarios para que todos los

empleados realicen sus funciones. La instalación de cualquier otro software puede afectar el

rendimiento y confiabilidad de los elementos provistos por la empresa.

Algunos peligros del uso de software no autorizado son:

Algunos juegos y protectores de pantalla personalizados han demostrado interferir con

la operación normal del software provisto por la empresa. Estos programas pueden

alterar la configuración de los sistemas lo cual puede causar funcionamiento deficiente.

Cualquier tipo de software diseñado para permitir actividades de intercambio de

archivos (“peer-to-peer”) de usuario a usuario, como por ejemplo Napster, Morpheus,

Kazaa, etc., es comúnmente utilizado para compartir/descargar archivos de música y

video. Este tipo de software ha demostrado ser particularmente propenso a fallas de

seguridad – facilitando la potencial divulgación de datos confidenciales y propagación

de virus. El uso de dicho software puede también exponer tanto al individuo como a la

empresa a riesgo de incumplimiento de las leyes de la propiedad intelectual.

Los mensajes instantáneos no provistos por la empresa usualmente utilizan canales de

comunicación que no están bien protegidos o controlados. Por esta razón convierten a

la computadora del usuario en un objetivo vulnerable para el ataque desde Internet y

más susceptible a infecciones de virus y otras clases de software maligno.

Cualquier software gratis que puede descargarse de Internet debe ser considerado como

potencialmente peligroso. Tal software podría causar daños o interferir con el correcto

funcionamiento del software legítimo instalado en la computadora. En algunos casos, este

software maligno puede ser usado para vulnerar la computadora – haciéndola vulnerable a

acceso por parte de individuos no autorizados. Estas computadoras vulneradas a su vez

podrían ser utilizadas para lanzar ataques adicionales contra las redes de Manpower o contra

otras computadoras conectadas a Internet.

Acuerdos de licenciamiento de software

Política

Las licencias de todos los productos de software provistos por Manpower son propiedad de la

empresa. Los empleados y otros usuarios autorizados pueden utilizar el software dentro de los

límites y condiciones especificados en los contratos de licencia. Los usuarios autorizados no

pueden hacer o distribuir copias de ningún software provisto por la Empresa.

Propósito

El objeto de esta política es evitar que los empleados de Manpower violen los términos y

condiciones especificados en los acuerdos de licenciamiento para usuarios finales de software

provisto por la Empresa.

Recomendaciones e información adicional

El Software está protegido bajo la ley de propiedad intelectual. Se consideran violaciones a tal

ley las siguientes acciones: instalar software de licencia individual en múltiples computadoras,

hacer copias del software sin permiso expreso o utilizar software de marca registrada sin su

correspondiente licencia según la versión utilizada. El incumplimiento del contrato de licencia

puede causar imposibilidad de uso, confiscación del equipo, multas o incluso pena de prisión.

Todos los empleados son responsables por el cumplimiento de todos los términos de uso para

todas las licencias de software.