**Políticas de seguridad para empresas y organizaciones**

En el siguiente documento se nombran y describen las políticas de seguridad recomendadas por malware-tec para asegurar tanto la privacidad, confidencialidad y disponibilidad de la información que se maneja en la empresa, así como la seguridad de bienes materiales e intelectuales, políticas que los empleados y colaboradores deben cumplir de manera satisfactoria.

* **Política de contraseñas seguras**

Se dice que una contraseña se considera segura cuando esta consta de al menos 10 dígitos, utilizando mayúsculas, minúsculas, números y signos especiales, se recomienda no utilizar la misma contraseña para diferentes cosas como lo pueden ser redes sociales, correos electrónicos, cuentas bancarias, computadoras, teléfonos celulares, etc., además de evitar usar datos personales como los son fechas de cumpleaños. Nombres de parejas, familiares, mascotas, gustos personales, etc.

* **Política de manejo adecuado de credenciales**

En ocasiones es complicado recordar las contraseñas que constan de varios dígitos y diferentes símbolos sin embargo se debe evitar anotar las credenciales como el nombre de usuario y la contraseña en papeles o notas adhesivas ya que estas pueden ser vistas por personas ajenas a la organización y puede presentar un alto grado de riesgo para la información manejada e infraestructura de la red.

* **Política de descarga de software**

Queda estrictamente prohibido que los empleados o colaboradores realicen descarga e instalación de algún tipo de software en los equipos pertenecientes a la empresa ya que esto pude desencadenar la infección por malware, se recomienda que cuando se necesita hacer una nueva instalación de algún programa esta sea realizada por el personal de TI con activación de claves originales evitando utilizar cracks para la activación.

* **Política de seguridad en los dispositivos de red**

En una red de datos es obligatorio hacer configuraciones de seguridad a los diversos equipos de red como lo pueden ser los routers, switches, módems o los mismos equipos de cómputo.

Existe una variedad de configuraciones como lo pueden ser: generar contraseñas de accesos a las configuraciones de estos equipos, seguridad en los puertos de switch o del router, listas de control de acceso, etc., se recomienda que estas configuraciones sean realizadas por personal con experiencia en el tema para preservar la seguridad de estos equipos de red.

* **Política de correo electrónico seguro**

Esta política de privacidad hace alusión a la seguridad que se debe considerar para el uso de correos electrónicos, cuando se reciban correos nuevos, verificar que conozcamos al remitente que envía, no descargar ningún tipo de archivo adjunto que no hallamos solicitado y de la cual desconozcamos al remitente, en caso de descargar algún tipo de archivo adjuntado, escanearlo con el antivirus instalado en la computadora para descartar una posible infección de malware.

* **Política de detección de ingeniería social**

los ataques de ingeniería social se da cuando una persona ajena a la empresa se hace pasar por alguna otra persona u organización con la finalidad de obtener algún tipo de información privada y confidencial, este tipo de ataques se pueden llevar a cabo a través de llamadas telefónicas, correos electrónicos, mensajes de texto o inclusive de manera física, en caso de encontrarse ante un posible ataque de este índole lo recomendable es verificar la información que el atacante ofrece con personal que este al tanto de tramites que se tengan pendientes.

* **Política de restricción de equipos de red y computo**

los equipos de cómputo y de red de la empresa no solo deben estar protegidos de manera lógica, si no, también de manera física, es decir, solo el personal autorizado debe tener acceso a estos, evitar a toda costa que personas ajenas a la empresa manipules equipos de cómputo como de red, así también limitar a los propios empleado a utilizar únicamente los equipos a los cuales estos tienen permisos de utilizar (por ejemplo: un empleado de administración no debe tener acceso a equipos de red como switch, routers o servidores).

* **Política de privacidad en proyectos futuros y actuales**

Los trabajadores no pueden dar información sensible de los proyectos tanto actuales como futuros a personas ajenas a la empresa, como lo pueden ser miembros del equipo, funcionamiento, errores, posibles ideas de proyectos, etc.

* **Política de manejo de archivos físicos**

En cuanto a archivos físicos se refiere los empleados no pueden substraer archivos, carpetas, documentos, etc., fuera de la empresa a excepción de contar con el permiso del jefe inmediato, así como no pueden acceder a estos activos sin el permiso necesario, así también queda prohibido sacar copias o fotografías a documentos con información critica.

* **Política de seguridad en dispositivos de almacenamiento externo**

Queda estrictamente prohibido conectar a equipos de la empresa dispositivos externos como lo pueden ser memorias de almacenamiento USB, SDcard o CD´s que hayan sido encontrados en lugares públicos (estacionamientos, calles, etc.) ya que pueden ser portadores de malware que puedan poner en riesgo la información almacenadas en los equipos.

* **Política de mantenimiento preventivo a equipos de computo**

se debe de establecer un periodo para la realización de mantenimiento preventivo a equipos informáticos de la empresa con la finalidad de evitar posibles fallas futuras para así preservar el ritmo de producción

* **política de nuevos usuarios a la red empresarial**

queda prohibido dar acceso a la red tanto cableada como wifi a usuarios ajenos a la empresa, a excepciones de contar con el permiso correspondiente de altos directivos, en caso de ser permitido se aconseja em monitoreo del tráfico de la red para evitar posibles prejuicios de un agente externo

* **política de software de seguridad**

se recomienda altamente el uso de software de seguridad en la red como lo son antivirus(activados con claves originales), IDS e IPS, firewall, etc., según los requerimientos de la red con la finalidad de aumentar el grado de seguridad dentro de la misma.

* **política de actualización de sistemas operativos**

se establece que el equipo de TI tiene que estar al tanto de las actualizaciones de los sistemas operativos para que estos se mantengan al día con los parches de seguridad ofrecidos por la empresa desarrolladora, esto con la finalidad de evitar que se presenten vulnerabilidades en estos activos.

* **política de control de acceso físico a equipos de red**

solo el personal autorizado tiene acceso al cuarto de telecomunicaciones o también llamado SITE donde se encuentra todo el equipo de red que mantiene la infraestructura (como los son switch, routers, módems, etc.), esto con la finalidad de evitar saboteos tanto de agentes internos como externos

* **política de configuraciones de seguridad**

el personal e TI debe tener en cuenta configuraciones de seguridad en los equipos como lo son ACL, desactivación de puertos inactivos, seguridad en puertos, implementación de contraseñas de seguridad para las diferentes interfaces de administración, etc., evitando a toda costa dejar configuraciones y contraseñas por defecto en estos equipos

* **política de accesos a painas web**

queda restringido la visita a páginas web ajenas a las tareas que desempeña el colaborador como lo pueden ser páginas de pornografía o alguna otra que interrumpa el desempeño de este, además se evitara que páginas con contenido malicioso infecten los equipos de la empresa.

* **política de realización de backups**

el personal de TI debe determinar un periodo para la realización de backups tanto del sistema operativo como de los archivos que se encuentran en las computadoras de la empresa con la finalidad de evitar perdida de información en caso de desastres naturales o ataques informáticos.

* **política de cifrado de información**

se recomienda hacer uso de software de cifrado de los datos que se tengan almacenados en los equipos de cómputo con la finalidad de que estos no sean visibles a personas ajenas a la empresa en caso de presentar se un robo de información.

* **política de implementación de UPS (para actuar ante fallos eléctricos)**

se recomienda el uso de equipo como UPS para evitar daños a equipos de cómputo, así como perdida de información en horarios laborales en caso de presentarse picos de corriente eléctrica.

* **política de inventario de equipos que constituyen la red de datos**

es recomendable que se tenga un inventario de los equipos que constituyen la red para tener un control más establecido en caso de perdida.

* **política de descargas seguras de documentos de internet**

todo documento descargado de internet debe ser de páginas seguras y posteriormente analizados en busca de malware por el antivirus instalado, para así evitar la infección de los equipos.