La seguridad informática ha cobrado una relevancia especial debido a las exigencias actuales que requieren cambios tanto en tecnología como en los sistemas de información. La aparición de nuevos virus y sistemas de intrusión ha hecho que las empresas sean vulnerables a ataques en sus sistemas. Por esta razón, se han desarrollado una serie de directrices que orientan a los usuarios de los sistemas de **SERVILIN LTDA**. para prevenir dichos ataques y preservar la confidencialidad de la información.

Este documento contiene una serie de normas de obligatorio cumplimiento, avaladas por la Gerencia, para el uso de los recursos informáticos. El incumplimiento de estas normas acarreará sanciones disciplinarias.

1. MANEJO DE HARDWARE (EQUIPOS)

- El proceso TIC es el principal responsable del buen funcionamiento de los equipos de cómputo y es el único autorizado para realizar mantenimientos y mejoras, como cambios de procesador, memoria o tarjetas. No se permite que personal ajeno a este departamento manipule el computador, y está prohibido destapar el equipo.

- Está prohibido marcar el equipo o colocar cualquier tipo de calcomanía o sticker no autorizado.

- Los equipos solo pueden ser trasladados con la aprobación del proceso TIC y el aval de Seguridad y salud en el trabajo, con el fin de controlar los riesgos derivados en las actividades laborales.

- El colaborador debe de informar la pérdida o daño del equipo que tengan a su cuidado y que sea propiedad de SERVILIN LTDA.

- La conexión de equipos personales está totalmente prohibida; si es necesario, debe contar con la aprobación del proceso TIC y de la Gerencia.

- Se recomienda que los equipos cuenten con estabilizadores o supresores de picos para disminuir la posible pérdida de información por cambios de voltaje y, de ser posible, estar conectados a tomas reguladas de corriente eléctrica.

- Los parlantes serán retirados de los puestos de trabajo, salvo aquellos que se utilicen para funciones estrictamente laborales, los cuales serán monitoreados por el proceso TIC.

- Está prohibido el consumo de alimentos en los puestos de trabajo.

- Al crear un nuevo puesto de trabajo o al retirar a un colaborador de la empresa, el jefe inmediato deberá informar al proceso TIC para realizar la respectiva inspección, recibir el equipo y la información que este contiene.

- Está totalmente prohibido el uso de pendrives (USB) y discos duros externos personales; solo se deben utilizar aquellos que hayan sido solicitados debidamente al proceso TIC y a la Gerencia.

2. MANEJO DE SOFTWARE (PROGRAMAS)

- Solo el proceso TIC será responsable de la instalación y puesta en marcha del software en los equipos. La adquisición de las licencias se realizará en coordinación con el proceso de compras y con la aprobación de la Gerencia.

- Se prohíbe estrictamente la instalación de programas no licenciados, así como el uso de cracks, keygens y programas de chat.

- El uso del internet debe ser estrictamente para fines laborales.

- La empresa proporciona un correo corporativo; por lo tanto, está totalmente prohibido el uso de correos personales en los equipos de la empresa, así como el uso de Google Drive, OneDrive y otras cuentas personales.

- Los sitios de internet prohibidos, que afectan el rendimiento de la red, incluyen: bibliotecas musicales, canales de radio y televisión, páginas de descarga masiva y torrents, así como sitios relacionados con pornografía, violencia, drogas, hacking, phishing, spam, piratería y redes sociales como Twitter, Facebook, Sónico, MySpace, Instagram, entre otros.

- El uso de internet será monitoreado constantemente para verificar que se utilice adecuadamente.

- Cada equipo debe contar con fondos de pantalla corporativos, los cuales no se pueden cambiar ni modificar.

- Los equipos tendrán un bloqueo automático programado.

3. CLAVES DE SEGURIDAD

- Todos los equipos deben tener una contraseña asignada por el proceso TIC, El usuario tiene prohibido modificar o hacer cambios en las contraseñas establecidas. En caso de hacerlo, debe informar de inmediato al proceso encargado de controlar los cambios en las contraseñas, según el tiempo estipulado y los requerimientos de seguridad.

- La contraseña debe de incluir mayúsculas, minúsculas y números para establecer un mayor nivel de seguridad.

- La utilización de la contraseña es personal e intransferible. Cada usuario debe memorizarla y está completamente prohibido compartirla con terceros o compañeros de trabajo.

- Se deben escoger caracteres fáciles de recordar, que preferiblemente se puedan digitar sin mirar el teclado y de forma rápida, pero que no sean palabras comunes ni nombres propios de familiares o allegados.

- Por seguridad de la información, se debe cambiar la contraseña cada 3 meses, previo aviso al proceso TIC.

- Los documentos digitales que cuenten con importancia relevante dentro de cada uno de los procesos deben contar con contraseña de apertura, que será gestionada por cada proceso.

4. CONTROL Y USO DE LA EXTRACCIÓN DE INFORMACIÓN

- El uso de puertos extraíbles y sistemas de grabación digital están totalmente prohibidos. Solo los jefes de departamento o las personas que lo requieran por su trabajo, con previa autorización de la Gerencia, tendrán acceso a estos.

- La información digital que salga de la empresa solo se podrá utilizar con el correo electrónico corporativo.

- El encargado del proceso TIC será el único responsable de realizar las copias de seguridad; en ningún momento, ninguna otra persona podrá realizarlas.

- El proceso TIC sincronizará en cada computador una carpeta compartida en Drive o OneDrive, donde se guardará la información relevante de la empresa. Esta carpeta tendrá una copia de seguridad según los términos establecidos. Si se almacena información en otro lugar, será bajo la responsabilidad del usuario.

- Los backups se realizarán cada 15 días y una vez al mes de manera total. Serán guardados en dispositivos extraíbles o serán cargados en la nube para su respectivo almacenamiento.

- Los equipos se podrán utilizar solamente en la jornada laboral estipulada en el contrato de lunes a sábado. En caso de necesitar trabajar en tiempo extra, los domingos o festivos, es necesario enviar un correo electrónico al proceso TIC y gerencia solicitando autorización. Solo los equipos de seguridad electrónica y los servidores trabajarán 24 horas al día, los 7 días de la semana, incluyendo los de monitoreo y cámaras.

- Los usuarios de la red que necesiten trabajar de manera remota, es decir, mediante escritorio remoto, deben solicitar autorización vía correo electrónico al proceso TIC y gerencia.

Estos mecanismos de control y seguridad, dispuestos por la Gerencia, se implementarán a partir de la presente fecha y serán notificado a cada uno de los trabajadores.

_____

DANCERI LÓPEZ JARAMILLO
REPRESENTANTE LEGAL
20/06/2024