

Escritorios Limpios: Buenas Prácticas de Seguridad

Entorno de trabajo

- Almacenamiento de información:
 - Guarda únicamente información pública en sitios de acceso público.
 - Mantén el entorno libre de documentación sensible.
- Seguridad informática:
 - Actualiza el software regularmente y aplica los parches de seguridad según las políticas institucionales.
 - Utiliza programas antivirus y antimalware reconocidos y actualizados.
 - Realiza copias de seguridad (backups) periódicas, siguiendo las políticas de seguridad, y almacénalas en un entorno distinto al de uso diario.
 - Verifica la efectividad de los backups mediante pruebas de recuperación periódicas.
- Accesos remotos:
 - Usa VPN y conexiones seguras para acceder a información crítica de manera remota.
 - Evita redes Wi-Fi públicas; si no hay alternativa, utiliza una VPN para proteger la información.
- Control de accesos:
 - Bloquea automáticamente la pantalla de tu computadora con una contraseña cuando no estés presente.
 - Cierra las sesiones en los sistemas al dejar de utilizarlos o si otra persona necesita usar tu equipo.
- Manejo de información:
 - Verifica la información recibida por canales no habituales para evitar decisiones basadas en datos falsos.

Orden y limpieza en el espacio de trabajo

El concepto de "escritorio limpio" no solo implica mantener un entorno organizado, sino también proteger la información sensible o confidencial. Es fundamental adoptar hábitos que eviten la exposición de datos institucionales a personas no autorizadas.

En nuestras oficinas manejamos información sensible que, en malas manos, puede tener consecuencias negativas para la institución. Todo documento o dato dejado a la vista representa un riesgo, especialmente en áreas de acceso compartido o donde pueden ingresar personas externas.

Recomendaciones: Si debes ausentarte de tu oficina:

- Bloquea la pantalla de tu equipo con contraseña.
- Cierra la sesión en los sistemas que no estés utilizando.
- Protege tus contraseñas; no las escribas ni las dejes visibles cerca de tu equipo.
- Guarda dispositivos de almacenamiento removibles en lugares no accesibles ni visibles.
- Asegura objetos personales, como billeteras o carteras, en muebles seguros.

Al término de la jornada laboral:

- Verifica que todos tus dispositivos (computadoras, notebooks, móviles) tengan contraseñas activadas.
- Ordena el escritorio y organiza cables sueltos para evitar accidentes.
- Mantén el espacio libre de líquidos que puedan dañar tus equipos.
- Limpia pizarras o pantallas utilizadas en reuniones para eliminar cualquier información sensible.

Sugerencias permanentes:

- Documentación sensible:
 - Guarda documentos con datos confidenciales (como información de estudiantes, contratos o claves) en muebles con llave.
 - Evita dejar documentos sensibles sobre el escritorio si no los estás usando.
 - Destruye de forma segura cualquier documento confidencial antes de desecharlo.
- Dispositivos electrónicos:
 - Asegura notebooks, tablets y otros dispositivos en lugares seguros para prevenir robos.
- Limpieza y organización:
 - Dedicar un día a limpiar y organizar tu espacio de trabajo. Esto no solo mejora la estética, sino también la seguridad y el rendimiento de los equipos al reducir el polvo acumulado.
- Impresoras:
 - Retira siempre los documentos impresos y guárdalos inmediatamente si contienen información sensible.

Mantener un escritorio limpio y organizado no solo refleja profesionalismo, sino que también es un componente esencial de la seguridad de la información. Adoptar estas prácticas ayuda a proteger datos institucionales y personales, promoviendo un entorno laboral seguro y eficiente.