UNBOUND™

Guía de Tecnología

TABLE OF CONTENTS

1 Equipo físico

- Es posible que usar computadoras de la misma marca pueda simplificar el mantenimiento y soporte.
- A partir del 24 de enero, 2020, Windows 7 ya no es soportado por Microsoft. Se recomiende actualizar las computadoras a Windows 10. El acceso de internet con Windows 7 ya no es seguro.
- Con Windows 10, se recomiende un mínimo de 8 GB de RAM.
- Al mínimo, se recomiendan los procesadores en la serie "i," por ejemplo, Intel Core i5, i7, etc. No se recomiendan los procesadores más antiguos como Pentium.
- Se recomienda configurar Windows para aplicar las actualizaciones de Windows automáticamente. Debe haber un sistema de verificación para asegurar que las actualizaciones se apliquen a cada computadora, aunque sea una verificación manual de cada una.
- Mantener un inventario de todas las computadoras.
- Cuando los discos duros dejen de funcionar o se desechen, tomar precauciones para destruirlos (no solo eliminar la información sino destruir físicamente los discos duros, por ejemplo, por cortarlos en tiras para que la información no se pueda acceder). Cualquier paso que haga que el disco duro no funcione y no sea accesible es suficiente. Si se usa un vendedor para hacer esto, solicitar ver el proceso de destruir los discos duros o solicitar documentación que muestra lo que se hizo.

2 Acceso de usuarios

- Asegurarse que todas las computadoras sean protegidas por contraseña. Si varios usuarios usan la misma computadora, cada usuario debe tener su propia contraseña para la computadora. Las contraseñas no deben ser compartidas entre los usuarios.
- Crear una política de la complejidad de las contraseñas, por ejemplo, requerir que las contraseñas tengan una mezcla de letras mayúsculas y minúsculas, dígitos, etc.
- Requerir que las contraseñas sean cambiadas con regularidad, por ejemplo, cada 90 días.
- Considerar solo permitir que ciertos usuarios tengan acceso administrativo a las computadoras si es necesario. Si cualquier usuario tiene acceso administrativo en su computadora, revisar las computadoras con frecuencia para asegurar que los programas descargados sean apropiados y necesarios para el trabajo en Unbound.
- Considerar crear una política que disuade los usuarios a usar el Internet por asuntos personales. Sitios web específicos o inapropiados se pueden prohibir si es necesario. Revisar ocasionalmente el historial de navegación para asegurar que sitios web inapropiados no sean accedidos, ya que esto puede crear la posibilidad de descargar algo maligno.
- Considerar brindar capacitación general de computación a los usuarios, por ejemplo, en Windows o programas específicos.

3 Red

- Si se usa una red para conectar las computadoras, hacer una auditoría de la conexión de la red regularmente para asegurar que nadie la esté usando que no sea el personal de Unbound. Cuando alguien se va de Unbound, terminar su acceso a la red.
- Si se usa una red, usar un cortafuegos para prevenir el acceso no autorizado.
- No conectar a redes públicas no confiables, por ejemplo, redes inalámbricas disponibles en cibercafés o aeropuertos usando computadoras ni cuentas de Unbound. Por ejemplo, no acceder a una cuenta de correo electrónico de Unbound usando una red pública no confiable. Es posible que otras personas accedan a la Información por redes públicas. Si se usa una VPN (Red Virtual Privada) confiable al conectar a redes públicas, en ese caso es posible que la conexión sea segura.

4 Copias de seguridad

- Se debe realizar una copia de seguridad de los datos, según su importancia, según la criticalidad para sus operaciones. Hacer preguntas como, “¿Si perdiéramos estos datos, ¿cuál sería el daño? O “¿Por cuánto tiempo podemos trabajar si de repente nuestros sistemas dejan de funcionar o perdemos datos?” o “¿Con qué frecuencia cambian estos datos?” Las respuestas a preguntas así les ayudarán a decidir con qué frecuencia deben realizar copias de seguridad.
- Un servicio de almacenamiento en línea como Microsoft OneDrive o Google Drive podría ser una buena opción que no requiere mucha configuración técnica. Esto es recomendado más que unidades USB u otras unidades externas porque estas están sujetas a fallas de hardware.
- Revisar manualmente y a menudo las copias de seguridad para asegurar que el proceso que haga la copia de seguridad esté funcionando bien (que los datos no estén corruptos ni inutilizables).

5 Internet

- Al trabajar en línea, siempre asegurar que el URL/la dirección del sitio web use “https” en vez de “http”. La s indica que es un sitio seguro.
- No compartir contraseñas de sitios web con otros usuarios. Cada persona debe tener su propia y única contraseña.
- Cuando esté disponible y el costo no sea prohibitivo, comprar una conexión de internet suficiente rápida para evitar que los usuarios tengan demoras con su trabajo en línea.

6 Software de Antivirus

- Hay muchas aplicaciones de antivirus que funcionan bien.
- Si se usa una red, la clave es tener una administración centralizada de las computadoras en la red para prevenir malware (programas malignos) y para poder recibir notificaciones en el caso de una amenaza. En una red con administración centralizada, es posible verificar remotamente cuáles computadoras están actualizadas.
- Si todas las computadoras son independientes en vez de conectadas a una red, es crítico configurar el software de antivirus para actualizar automáticamente. Con computadoras independientes, es necesario revisarlas regularmente para asegurar que estén actualizadas.
- Si una computadora está infectada y el software de antivirus no elimina o previene bien el problema, sería ideal apagar la computadora, desconectarla de la red e instalar nuevamente el sistema operativo. Si el software antivirus detecta el problema, es una buena idea escanear nuevamente la computadora para asegurar que no haya más amenazas.
- Para computadoras con Windows 10, “Windows Defender” está incluido con Windows 10 y es una buena solución sin un costo adicional. Para una red con una administración centralizada, es posible que soluciones empresariales sean una mejor opción. Dependiendo de cuáles opciones están disponibles en cada país, podrían ser una opción compañias como Eset, McAfee, Kaspersky, u otras (favor de consultar su vendedor de tecnología local para determinar cuáles soluciones están disponibles en su país).

7 Otro Software

- Asegurar que todas las licencias de software, incluso Microsoft Windows, sean legales. Es posible que Microsoft ofrezca descuentos para organizaciones sin fines de lucro al contactarle en Microsoft.com
- Mantener un inventario de todas las licencias de software para asegurar que todas las copias sean legales.
- El software debe estar actualizado regularmente y la versión no debe ser más antigua que la segunda versión más reciente disponible y todavía soportado por el vendedor. Por ejemplo, si el vendedor de software ha publicado la versión más reciente de 5.4 y las versiones anteriores son 5.3, 5.2 y 5.1, la versión en cualquier computadora debe ser al menos 5.2.
- Restringir el acceso de software personalizado a solo los usuarios que lo necesitan. Asegurar que cada usuario tenga una cuenta y contraseña únicas que no sean compartidas con otros usuarios.

8 Privacidad de Información

- Para la Información de empleados guardada digitalmente o de manera física, asegurar que solo está disponible al personal que necesita acceso a esta Información. Tomar precauciones para proteger los datos. Los datos guardados digitalmente deben ser protegidos por contraseña. Datos guardados de manera física deben estar cerrados seguramente con llave.
- La información personal de padrinos que visitan el proyecto debe ser protegida y accedida solo cuando sea necesario. Después de completar un viaje, esta información debe ser eliminada (si es digital) o destrozada y desecha (si es física).
- Si hay regulaciones de la privacidad de información específicas a su país, asegurar de cumplir con ellas (por ejemplo, en Estados Unidos, tenemos que guardar los datos de tarjetas de crédito de maneras muy específicas).

9 Mantenimiento de Computadoras

- Si una computadora está funcionando más lentamente que lo esperado, es posible usar el Administrador de tareas de Windows para ver cuales aplicaciones están usando los recursos de la computadora. Es posible que sea necesario reinstalar el sistema operativo de una computadora si los usuarios siguen enfrentando dificultades. Si se ocupa 90% o más del espacio del disco duro, el desempeño de la computadora empeorará y es posible que eliminar archivos para desocupar espacio ayude el desempeño.
- Los conductos de aire de las computadoras deben estar despejados. En ambientes con mucho polvo, es posible que sea necesario limpiar el interior de las computadoras.
- Es posible dejar prendidas las computadoras durante la noche pero los usuarios deben cerrar sesión y dejar la computadora en la pantalla de iniciar sesión de Windows. Reinciar la computadora diariamente es la mejor práctica ya que se realiza al principio del día o al fin del día al cerrar sesión.

10 Seguridad de información y el uso de correo y teléfonos celulares

- Nunca hacer clic en un enlace ni abrir un dato adjunto de un correo si no es completamente seguro que el enlace o el dato adjunto es seguro. Hacer clic en estos puede dejar que una persona maliciosa gane acceso a la red o a información confidencial o puede infectar la red con un virus.
- Avisar a las familias qué información pueden esperar recibir de Unbound por teléfono celular o correo, por ejemplo, una eCarta o una solicitud de una foto y cómo aparecen estos mensajes. Avisarles que si reciben otros mensajes (por ejemplo, una solicitud para reunirse o información personal o de la cuenta de banco), que no deben responder. Deben contactar al personal de Unbound para reportar la solicitud.
- No aceptar llamadas ni hacer clic en enlaces en mensajes de personas no conocidas.
- Revisar la configuración de privacidad en WhatsApp – controlar quienes pueden ver su foto, estado y otra información.
- Animar a los papás que revisen la actividad del celular de sus hijos y que hablen con ellos sobre la seguridad.