Universidad Veracruzana

Seguridad en trabajo desde casa

Información segura... ¡es cultura!®

Seguridad en trabajo desde casa

El trabajo desde casa ha crecido de forma acelerada a nivel mundial en los últimos meses, convirtiéndose para muchas empresas e instituciones en una forma de trabajo esencial para continuar su operación.

Esta modalidad conlleva el uso de computadoras, dispositivos móviles como laptops, celulares o tabletas para leer y/o enviar correos electrónicos, acceder a sitios web, entre otras actividades derivadas de nuestra labor en una institución.

Es por ello que si bien permite y coadyuva a la continuidad de un negocio o de una institución, también existen riesgos que pueden afectar la seguridad de la información por lo que es imprescindible que se implementen ciertas medidas de seguridad y mecanismos de control con la finalidad de garantizar un trabajo en casa seguro, los cuales se abordarán a continuación.

Riesgos de trabajo remoto o en casa

Existen diversos riesgos y amenazas que se pueden presentar al realizar el trabajo remoto y que pueden afectar la seguridad de la información de la institución entre los que se encuentran:

- El dispositivo de un usuario que no cuenta con herramientas de protección como un antivirus y además no tiene instaladas las actualizaciones de seguridad o se encuentra mal configurado.
- Phishing, técnica que utiliza el envío de correos electrónicos con el fin de engañar al usuario de una institución para obtener información confidencial como usuarios o contraseñas.
- El malware, como virus, troyanos, spyware, adware puede infectar a un dispositivo de un usuario que accede de forma remota a información institucional a través de:
  - Correo electrónico
  - Sitios web
  - Descargas
  - Uso compartido de archivos
  - Redes sociales
  - Medios extraíbles como USB
- Robo o pérdida de un dispositivo
- Fugas de información.

Es importante que todo el personal y todos los usuarios de una organización o institución conozcan estos riesgos y que implementen los controles de seguridad adecuados que se mencionan a continuación.

Seguridad en trabajo desde casa

Controles de seguridad para un trabajo seguro en casa

•**Aplicación de las actualizaciones de seguridad de sistemas operativos y aplicaciones**: Es importante que tanto computadoras como dispositivos móviles tengan instaladas las actualizaciones más recientes del sistema operativo así como de todas las aplicaciones, siendo las más críticas las del antivirus, antimalware, las de acceso remoto, navegadores, clientes de correo electrónico y mensajería.

•**Contraseñas robustas**. Utilizar contraseñas fuertes, sin que se repita la misma en más de un servicio, usando un mínimo de 8 caracteres combinando letras mayúsculas, minúsculas, números, caracteres especiales, etc.

•**Estar alerta a los correos fraudulentos**: Usar el sentido común, ser precavido y cauteloso al revisar los correos electrónicos es fundamental, debiendo poner atención para identificar correos maliciosos que generen un sentido de urgencia, que estén mal redactados o con faltas de ortografía, sin abrir enlaces o archivos adjuntos sospechosos.

•**Configurar el bloqueo de sesión**. Esto impide el acceso al equipo después de estar inactivo durante cierto tiempo, por ejemplo, 2 minutos.

•**Cifrar los medios de almacenamiento**. En caso de robo o pérdida, este control permite proteger los datos de la organización o institución de posibles accesos malintencionados y garantizar la confidencialidad e integridad.

•**Limitar las capacidades de red en dispositivos móviles**. Deshabilitar el bluetooth o en su caso configurar el servicio con contraseña. Es importante ser cuidadoso con las redes wifi abiertas, priorizando en estos casos el uso de redes móviles.

•**Copias de seguridad**. Se debe contemplar realizar copias de seguridad de la información que se tenga en los dispositivos que acceden de forma remota, debiendo asegurar que las comunicaciones que transportan esos datos deben ser cifradas para garantizar su integridad. Asimismo, la copia de seguridad debe ser cifrada.

•**Conexión segura**. Cuando el usuario requiera acceder de forma remota a información que se encuentra en una o más computadoras de la red institucional, se utilizará una VPN - Red privada virtual que permite que el acceso sea seguro. Para acceder a la conexión segura, el usuario debe autenticarse con un nombre de usuario y contraseña e incluso se puede agregar un doble factor de autenticación.

Seguridad en trabajo desde casa

De esta forma se crea un canal cifrado entre el equipo y la red institucional para un intercambio seguro de información.

Al respecto, la Universidad Veracruzana cuenta con un Reglamento de Seguridad de la Información, en el que se plasman en su artículo 33, [Ref. 2] las medidas de control que se deberán implementar cuando se haga uso de las tecnologías de información que proporciona la Universidad fuera de las instalaciones universitarias, las cuales son:

I. Solicitar el acceso a través de una Red Privada Virtual mediante el Procedimiento de Servicios de Red publicado en el portal institucional;
II. Salvaguardar la información conforme a lo establecido en el Reglamento y leyes aplicables en la materia.

Referencias:

1. Incibe, Ciberseguridad en el teletrabajo
https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf

2. Universidad Veracruzana, Reglamento de Seguridad de la Información
https://www.uv.mx/legislacion/files/2019/12/Seguridad-de-la-Informacion-2019-Gaceta.pdf