Universidad de Valladolid

MEDIDAS DE SEGURIDAD EN EL TELETRABAJO

1. Compromiso de disposición del equipamiento y entorno adecuado

El trabajador utilizará preferiblemente los equipos puestos a su disposición por la UVa, si es el caso. De no ser así, se compromete a utilizar un equipo informático propio dotado de conexión a internet que disponga de los requisitos necesarios para poder conectarse a la red corporativa, según el procedimiento de conexión que se establezca.

Se debe contar con un espacio de trabajo adecuado para la prestación laboral mediante la modalidad de teletrabajo en lo que respecta a las condiciones ambientales, de iluminación, ergonomía, etc.

Si utiliza dispositivos como ordenadores portátiles o teléfonos móviles, manténgalos siempre bajo custodia. Si el equipo es extraviado o sustraído, comuníquelo inmediatamente a la Universidad.

2. Procedimiento de conexión y herramientas autorizadas

La conexión a los equipos de la UVa se hará exclusivamente siguiendo los procedimientos y medios establecidos para ello. No se realizarán conexiones con otros medios distintos a los especificados. La información con los procedimientos de configuración se encuentra disponible en el apartado “Acceso Remoto” de MiPortal y en Portal del Empleado de la web corporativa de la UVa.

Se utilizarán las herramientas de trabajo autorizadas o aquellas que sean imprescindibles para poder desarrollar su trabajo con normalidad. La instalación de software deberá hacerse exclusivamente de fuentes originales o de confianza. No se autoriza el uso de software de terceros que pueda comprometer la seguridad de los sistemas de la Universidad.

3. Condiciones generales del equipo de trabajo

El sistema operativo, aplicaciones ofimáticas, navegadores y todas las herramientas software instaladas en su equipo deben estar actualizadas y contar con los últimos parches de seguridad.

Deberá contarse con herramientas de detección de malware y antivirus para protegerse de amenazas. Estas herramientas deberán estar actualizadas y activadas en todo momento. Asimismo, se configurarán para realizar análisis periódicos.

La Universidad de Valladolid tiene a disposición de sus usuarios una serie de antivirus que puede descargar en MiPortal dentro de la opción “Descarga de Software”.

4. Seguridad en redes

Deberá contarse con una configuración del router wifi adecuada para asegurarse de que todas las medidas básicas de seguridad están establecidas.

Se evitará conectarse a redes wifi abiertas o públicas, ya que se desconocen las medidas de seguridad que tienen implementadas y quién puede estar conectado a ellas.

Se evitará la conexión desde equipos de uso público o compartido que no sean de su confianza, ya que estos pueden tener sus medidas de seguridad comprometidas.

5. Condiciones relativas al manejo de información

Evite descargar información corporativa en su dispositivo local. Si fuera necesario, mantenga las medidas de seguridad para evitar su acceso por terceros.

Se realizarán copias de seguridad en función del sistema de conexión utilizado. Cuando se trabaje con información en el equipo local, se realizarán copias de seguridad de la información en los equipos remotos de la Universidad. Cuando se trabaje directamente en remoto, en los sistemas de la Universidad, del mismo modo que lo haría habitualmente.

Puede proteger la información que tenga almacenada cifrando ficheros que considere que contienen información crítica o confidencial para la Universidad. Entre otros, un modo sencillo es el uso de software de compresión de archivos zip o similares con contraseña.

Elimine los datos o copias locales realizadas cuando dejen de ser necesarios. La información sensible o que contenga datos de carácter personal requerirá de un borrado seguro que evite su recuperación posterior. Puede utilizarse para ello el software de código abierto gratuito “Eraser” https://eraser.heidi.ie/download/ o soluciones equivalentes.

6. Credenciales de la Universidad

Extreme las precauciones en la custodia de credenciales. No las anote en un sitio visible, no las comparta y si sospecha que hayan podido ser sustraídas, proceda a cambiarlas de forma inmediata. Recuerde que la Universidad no le solicitará por correo electrónico o telefónicamente sus contraseñas. Si necesita cambiarlas, utilice MiPortal dentro de la opción “Mis Datos” en la tecla “Cambiar Clave”.

Evite almacenar en los navegadores información sobre contraseñas de manera automática. Borre los archivos temporales y el historial al finalizar la sesión de trabajo.

7. Protección de la sesión de usuario

Utilice una cuenta de usuario diferenciada del resto en su equipo doméstico, estableciendo una contraseña. Evite compartirla con otras personas con acceso al equipo.

Bloquee el terminal cuando no vaya a utilizar su equipo durante un tiempo. Adicionalmente puede configurar el bloqueo de sesión por inactividad en sistemas y aplicaciones.

Cuando inicie sesión en algún servicio corporativo utilizando un navegador web, recuerde cerrar la sesión al finalizar su trabajo para evitar accesos no autorizados.

Si su equipo cuenta con certificados personales, resulta imprescindible que el equipo esté protegido mediante usuario y contraseña.

8. Uso de soportes removibles y papel

Se evitará transportar información corporativa en unidades removibles como discos duros o memorias USB. En caso de necesidad, debe optarse por cifrar la información en dichos soportes para evitar el acceso no autorizado en caso de pérdida o sustracción.

Custodie los dispositivos en todo momento extremando las precauciones para evitar extravíos o sustracciones.

No etiquete los dispositivos removibles de forma que pueda reconocerse su contenido.

Se evitará imprimir o transportar información en soporte papel. En caso de necesidad, extreme las precauciones en su custodia para evitar pérdidas o sustracciones o accesos no autorizados.

9. Uso de correo electrónico

Para uso profesional, se utilizarán los buzones y direcciones de email corporativos. No se utilizarán servicios de email de uso personal. No redirija el correo institucional a servicios de terceros.

Cifre toda aquella información que contenga datos personales para su transmisión mediante el envío de correos electrónicos. La contraseña deberá proporcionarse al destinatario por un medio diferente al correo electrónico, por ejemplo, telefónicamente.

Evite descargar información corporativa en dispositivos propios. Si fuera necesario, mantenga las medidas de seguridad para que no sea accedida por terceras personas, cifrando la información mediante contraseña.

Preste atención a correos electrónicos de remitentes desconocidos o cuyo contenido pueda resultar extraño. Preste atención a adjuntos y a los enlaces contenidos en los correos electrónicos. Si sospecha, evite abrir archivos o seguir enlaces poco fiables. Elimine el correo y si lo considera de especial relevancia, comuníquelo a los informáticos de su centro o al CAU en la dirección soporte@uva.es.

Telefonía

El trabajador puede desviar las llamadas de su teléfono de trabajo a su teléfono personal, sin embargo, no está obligado a hacer uso de su propio terminal telefónico ni para recibir ni para realizar llamadas a terceros. Se utilizarán otros medios para ponerse en contacto con terceros, de preferencia, el email. Si resultase necesario, se pueden realizar llamadas mediante sistemas software de videoconferencia o llamadas de voz licenciados.

10. Videoconferencia y llamadas de voz

Deberán utilizarse los sistemas de videoconferencia licenciados por la Universidad. A este respecto, pueden utilizarse los sistemas Teams, Webex y Skype profesional. En el Campus Virtual tiene información y tutoriales sobre su uso.

11. Incidentes de seguridad

En caso de detectar que su dispositivo puede haber sido comprometido y la información institucional accedida o sustraída, deberá ponerse en contacto de manera inmediata con el servicio de informática de la UVa a través de la dirección soporte@uva.es.

12. Finalización de la situación de teletrabajo

Una vez concluya la modalidad laboral no presencial, el trabajador eliminará todos aquellos sistemas software y credenciales que permiten acceder a los equipos de la Universidad de manera remota. Del mismo modo, eliminará la información almacenada con motivo de la prestación laboral que la originó. Cuando se trate de información sensible o datos personales, el borrado se realizará de manera segura.

13. Información adicional

Para más información, puede consultar las preguntas frecuentes del INCIBE en el Anexo ¿Cómo trabajar desde casa de forma segura?

Si tiene cualquier duda o problema, escriba a los informáticos de su centro o al CAU, a la dirección soporte@uva.es.

Anexo.-

¿Cómo trabajar desde casa de forma segura?

Según las recomendaciones del CCN-CERT, las medidas a tomar para el teletrabajo son:

Pon a punto tu dispositivo para trabajar con él

- Instala una herramienta antivirus para protegerlo de las posibles amenazas que puedan afectarle. Más información en: Ponte al día con lo virus informáticos.
- Actualiza el sistema operativo así como el resto de programas, navegadores, aplicaciones o herramientas que tengas instalados en él a su última versión. Más información en: Actualízate junto a tus dispositivos.
- Crea una cuenta de usuario diferente en el dispositivo para separar tu espacio de trabajo personal del profesional. Más información en: Haz uso de cuentas de usuario.
- Instala un Red Privada Virtual (VPN) para crear una conexión privada entre tu dispositivo y el servidor de la empresa. Más información en: ¿Para qué sirve una Red Privada Virtual y qué ventajas aporta?

Salvaguarda la información

- Realiza periódicamente copias de seguridad de la información que vayas generando o almacenando en el dispositivo para no perderla. Más información en: ¿Qué datos son recomendables proteger?
- Protege la información que tengas almacenada cifrando el disco duro, los directorios, carpetas o ficheros que consideres que contienen información más crítica y confidencial para le empresa. Más información en: Cifrado y almacenamiento seguro de ficheros paso a paso.

Sé cauto con las redes a las que te conectas

- Revisa la configuración del router wifi de casa para asegurarte de que todas las medidas básicas de seguridad están establecidas. Más información en: Tu router, tu castillo. Medidas básicas para su protección.
- Evita conectarte a redes wifi abiertas y/o públicas, ya que no conoces qué medidas de seguridad tienen implementadas, quién puede estar conectado a ella, ni cuáles son sus intenciones. Más información en: ¡Conexión gratis a la vista! ¿Conecto mi móvil?

Y de manera adicional…

- Activa tu sentido común y presta mucha atención a las noticias, mensajes, correos electrónicos o cualquier otra información que puedas recibir a través de los diferentes servicios que utilices para evitar ser víctimas de fraudes online o

descargar malware aprovechándose de técnicas de engaño, como es la ingeniería social.
- Si tienes cualquier duda o problema, escribe a los informáticos de tu centro o al CAU a la dirección soporte@uva.es, y desde ahí te ayudarán.

Más información:

- OSI: Oficina de Seguridad del Internauta
- INCIBE: Ayuda en Ciberseguridad