CIRCULAR INFORMATIVA
UNA-CIT-CIRC-003-2020

PARA: COMUNIDAD LABORAL UNIVERSITARIA

ASUNTO: CONSIDERACIONES TÉCNICAS Y GENERALES RELACIONADAS CON LA COMISIÓN INSTITUCIONAL DE TELETRABAJO DE LA UNIVERSIDAD NACIONAL

FECHA 01 DE JULIO DE 2020

Con el fin de orientar las acciones relacionadas con el teletrabajo en cuanto a tecnología y seguridad, condiciones ergonómicas, el uso de documentos, la información para realizar el trabajo, entre otros, se actualizan las denominadas “Consideraciones técnicas y generales relacionadas con la Comisión Institucional de Teletrabajo de la UNA.

a) Respecto a las condiciones tecnológicas y de seguridad

Las siguientes son una serie de medidas y valoraciones por tener en cuenta para lograr un escenario mínimo aceptable de seguridad informática, aplicado a las personas que se encuentran en la modalidad de teletrabajo.

Con ello se procura asegurar las credenciales de las personas usuarias de sistemas informáticos en general, las condiciones de acceso y empleo de esos sistemas, así como el uso de equipo tecnológico y los dispositivos finales orientados a llevar a cabo la labor diaria.

1. Contraseñas (*passwords*)

Respecto de este tema, lo siguiente:

- Las contraseñas deben ser de uso exclusivo de quien teletrabaja y, por ende, no deben ser compartidas con terceras personas.

- Utilice contraseñas de al menos 12 caracteres que contengan números, letras mayúsculas, letras minúsculas y caracteres especiales. Evite recurrir a

Tel. (506) 2277-3000
Apartado 86-3000
Heredia
Costa Rica
www.una.ac.cr

contraseñas simples, de fácil deducción, tales como nombres, fechas especiales (cumpleaños, aniversarios, etc.) y casos similares.

- Si maneja información sensible, valore habilitar un segundo factor de autenticación si se encuentra disponible, que le permita el ingreso a una facilidad tecnológica determinada. Este puede corresponder a un correo electrónico, un mensaje corto (SMS) mediante telefonía celular, o la utilización de *software* adicional tal como *Google Authenticator*.

- Cambie su contraseña de forma periódica, y resguárdela en un lugar seguro.

- Evite dejar contraseñas almacenadas de forma permanente en dispositivos como computadoras, tabletas, teléfonos, entre otros.

- Conozca, aprenda y lleve a cabo la configuración requerida para la recuperación de las contraseñas que necesita en su labor diaria.

2. Actualización del *software*

Esta actualización permite a los fabricantes habilitar o mejorar características propias del *software* que desarrollan y, a la vez, corregir defectos de funcionamiento o de seguridad informática que hayan sido detectados.

Al respecto, se recomienda tener presente al menos lo siguiente:

- Actualización permanente de los componentes de sistemas operativos de los computadores y dispositivos en general que se utilicen para atender las labores de la institución. Particularmente, la actualización de los sistemas operativos *Windows*.

- Actualización permanente del *software* utilizado cotidianamente. Como una lista mínima de estos: Office 365, *Teams*, *Zoom*, navegadores en general (*Chrome, Firefox, Opera*), productos de *Adobe* (*Acrobat Reader*), entre otros. Sin embargo, esto debe aplicar a todos los programas informáticos instalados en cualesquiera dispositivos que se utilicen por la persona teletrabajadora.

3. *Software* para protección informática

Es el comúnmente denominado *software* antivirus. No obstante, hoy en día este concepto debe ampliarse a un *software* de protección integral para el equipo de cómputo casero o empresarial, con capacidades de protección antivirus, *antimalware* (*software* malicioso), protección en la conexión a internet (*internet security*), entre otros. La idea consiste en tener una solución integral más allá de un antivirus tradicional, que cubre solamente un aspecto en particular.

En este sentido, los equipos institucionales podrán disponer de una licencia de *software* con las características anteriormente mencionadas, particularmente los equipos de cómputo de escritorio tipo *desktop* y *laptop*. En caso de que esta posibilidad no exista, se recomienda que la persona usuaria final posea una licencia comercial de un *software* de protección informática, de marca reconocida, que permita su actualización permanente.

4. Respaldo y cifrado (encriptación) de los datos, y confidencialidad de la información

La persona teletrabajadora debe, en términos generales, tomar las medidas pertinentes para resguardar los datos y la información relacionada con su labor, mediante el uso de dispositivos alternos para su resguardo; entre ellos, memorias USB y discos duros externos.

Se sugiere para la información crítica o confidencial de índole no pública, utilizar soluciones de cifrado de datos para que sea accesible solamente a la persona autorizada. Para este efecto, se mencionan al menos las soluciones de *Bitlocker* y *Veracrypt*.

Se indica que las contraseñas utilizadas para el proceso de cifrado no pueden ser recuperadas en caso de extravío.

Si se comparte el equipo de cómputo personal, se debe asegurar que los datos institucionales almacenados en el dispositivo respectivo se encuentren separados y con acceso restringido a terceras personas.

5. Accesos por red privada virtual (*VPN*)

En términos generales, las facilidades y los sistemas informáticos de la institución han sido implementados de tal forma que puedan utilizarse desde la internet. En los casos en que su uso se restrinja a lo interno de la universidad, se deberá atender los requerimientos y el procedimiento establecido para solicitar el servicio de *VPN*, el cual permitirá a la persona teletrabajadora ingresar a estos recursos de forma remota.

Los accesos *VPN* otorgados son de uso exclusivo de las personas autorizadas.

6. Utilización de *software* comercial no licenciado.

Por aspectos legales, la utilización de *software* comercial no licenciado, comúnmente llamado *software* pirata, no está permitida.

En el ámbito técnico, el uso de *software* pirata expone al computador o dispositivo electrónico a infectarse de *software* tipo *malware* (*software* malicioso), por lo que no debe utilizarse.

7. Internet compartido

En caso de compartir la internet con terceras personas, asegúrese de que la velocidad contratada no interfiera con las actividades teletrabajables asignadas. Asimismo, si varias personas utilizan la internet al mismo tiempo, cerciórese de que no se interrumpan los servicios en línea requeridos, particularmente los sincrónicos tales como videoconferencias, llamadas telefónicas o similares.

En caso de que tenga otros dispositivos con conexión a internet en su hogar, verifique que se encuentren con las últimas actualizaciones de *software* disponibles. Asimismo, todas las contraseñas originales o de fábrica de estos dispositivos deben ser cambiadas.

8. Sesiones virtuales

Para reuniones virtuales sincrónicas que utilicen soluciones tales como *Cisco Webex*, *Microsoft Teams*, *Zoom*, *Google Keep*, entre otros; tenga en cuenta al menos lo siguiente:

- Revise con anterioridad su conexión a internet y el estado del equipo que utilizará para la reunión.
- Intégrese a la reunión virtual de forma puntual, o algunos minutos antes.
- Para reuniones grupales, no distribuya de forma pública los enlaces de reunión o las contraseñas de ingreso al evento.
- Conozca a fondo la herramienta que se utilizará para la reunión convocada.
- Asegúrese de activar y desactivar la cámara y el audio en los momentos en que deba llevar a cabo este tipo de acciones.
- Aprenda a utilizar el resto de las facilidades asociadas: conversación en línea (chat), compartir pantalla, enviar archivos, etc.

9. Ingeniería social y acceso a sitios web desconocidos.

La ingeniería social pretende, mediante el engaño, obtener información confidencial de la persona usuaria, con el objeto de generar actividades relacionadas con estafas.

En este sentido, mantenga una actitud vigilante ante las llamadas telefónicas, los mensajes de texto y correos electrónicos, donde se solicite suministrar información de carácter privado: contraseñas, números de teléfono, números de cuentas bancarias e información sensible similar.

Ingrese solamente a sitios web reconocidos, y evite aquellos que muestran al menos recompensas, premios o la obtención de *software* ilegal, música o videos de forma gratuita. El *software* de protección informática es una buena herramienta que minimiza el riesgo ante este tipo de actividades.

10. Firma digital

En caso de requerir el uso de firma digital, habilítelo con suficiente antelación. De preferencia, aprenda a configurarlo siguiendo la guía que se encuentra en línea por parte del Sistema Nacional de Certificación Digital.

11. Plan B en caso de ausencia de fluido eléctrico o de la internet

En los casos de suspensión del fluido eléctrico o de la internet, valore las actividades que pueda llevar a cabo ante la ausencia de estos servicios, mientras se restablecen.

b) Respecto a las condiciones ergonómicas

1. La persona en teletrabajo le garantiza a la institución que dispone, al menos, de un escritorio, una silla ergonómica y otros requerimientos para la realización de su trabajo, en aras de la salud laboral.

2. Asimismo, deberá verificar que en su hogar no existan condiciones de riesgo asociadas que puedan traducirse en accidentes laborales o que afecten su salud, al cumplir con su trabajo fuera de la institución.

c) Respecto al uso de los documentos o la información para realizar el trabajo

1. La información institucional en archivos digitales deberá ser custodiada de forma segura, para evitar su utilización por parte de terceras personas. En concordancia con esto, se proveerá de mecanismos para encriptarla en caso de ser necesario, en función de la criticidad y privacidad de esta.

2. En caso de tener que trasladar información en físico desde la institución al hogar, para la continuidad del servicio, se deben establecer los mecanismos de control que permitan dar la seguridad respectiva.

Tel. (506) 2277-3000
Apartado 86-3000
Heredia
Costa Rica
www.una.ac.cr

3. La persona superior jerárquica deberá estar al tanto del tipo de información institucional que se estará accediendo desde el sitio de teletrabajo.

4. La persona teletrabajadora deberá tomar las previsiones necesarias para que la información universitaria sea de acceso restringido, evitando que sea compartida o del conocimiento de terceras personas ajenas a la institución.

5. En el equipo que se utilice para teletrabajar, se implementarán los mecanismos tecnológicos de *software* para verificar la conexión efectiva de la persona teletrabajadora con las redes institucionales durante la jornada de trabajo.

d) Otros aspectos por considerar

1. La persona superior jerárquica establecerá, acorde con su responsabilidad, la forma de seguimiento de las labores de la persona en teletrabajo.

2. La persona que teletrabaje deberá cumplir con las condiciones necesarias en materia de imagen y protocolo en caso de requerir acceso a la institución, mediante videoconferencia u otros medios similares.

3. El teletrabajo está asociado a la jornada y al horario de la persona, por lo que cualquier variación en forma permanente deberá ajustarse en la declaración jurada de horario. En caso de que el ajuste sea temporal y no consecutivo, se deberá formalizar mediante un documento de la persona superior jerárquica que justifique este cambio del horario en el día indicado.

4. En caso de teletrabajo por contingencia, una vez superada la situación que lo originó, si la persona desea continuar en esta modalidad, debe completar y entregar la adenda y el formulario de teletrabajo ordinario correspondientes.

Estamos en la mejor disposición de continuar promoviendo y dando consolidación al teletrabajo en la Universidad Nacional.

Se reitera que la documentación dirigida a la Cituna se está tramitando mediante el correo progteleuna@una.cr

Atentamente,

MARLY YISETTE ALFARO SALAS (FIRMA)
Firmado digitalmente por MARLY YISETTE ALFARO SALAS (FIRMA)
Fecha: 2020.07.01 09:56:18 -06'00'

Marly Yisette Alfaro Salas
Coordinadora

Tel. (506) 2277-3000
Apartado 86-3000
Heredia
Costa Rica
www.una.ac.cr