Universidad Estatal a Distancia

Rectoría

Dirección de Tecnología, Información y Comunicación

Vicerrectoría de Planificación

Programa de Teletrabajo

Diagnóstico sobre ciberseguridad entre las personas teletrabajadoras de la UNED

Mag. Adriana Oviedo Vega

Lic. Bryan Carranza Rodríguez

Mag. Johnny Saborío Alvarez

Mag. Alejandro Sanchez Rivera

Mag. Michael González Flores

Noviembre, 2020

Tabla de contenidos

Índice de gráficos

I. Justificación

Desde el año 2015, la Universidad Estatal a Distancia oficializó la modalidad de teletrabajo y desde entonces, ha ido incorporando más personas a esta opción de trabajo. Actualmente, en el 2020, la UNED cuenta con 355 personas teletrabajadoras y se proyecta que en un corto plazo se podría llegar a triplicar esta cantidad.

La modalidad de teletrabajo permite al colaborador realizar sus funciones desde otro lugar que no es la oficina de su dependencia, sino que las puede ejecutar desde su domicilio o inclusive desde otros lugares y países. El concepto etimológicamente significa trabajar a distancia.

No obstante, esa distancia requiere que la persona teletrabajadora utilice dispositivos tecnológicos para llevar a cabo sus tareas. Además, requiere de una conexión estable y segura que le permita acceder a la información almacenada en la nube, a servidores de la institución y con ciertas características para que ningún dato sea dañado, alterado o robado.

La ciberseguridad, según el sitio web (Kaspersky, 2020) es “la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica”.

Al cabo de 5 años de que la UNED cuenta con la modalidad de teletrabajo activa, se propone elaborar una Guía de buenas prácticas de ciberseguridad para toda su población de trabajadores, pero con especial énfasis en aquellas personas teletrabajadoras que podrían utilizar más variedad de dispositivos tecnológicos y acceder a la información desde puntos que podrían convertirse en amenazas para la institución.

Por esta razón, el Programa de Teletrabajo y la Dirección de Tecnología, Información y Comunicación decidieron elaborar un diagnóstico entre la población teletrabajadora de la UNED para determinar cuáles son las prácticas de este grupo de personas en temas como: claves de acceso, equipos tecnológicos, redes que utilizan, acceso y respaldos de la información y los hábitos que acostumbran realizar tanto con las terminales como con los datos.

Este diagnóstico permitirá ahondar en los puntos que se considerarían amenazas importantes para la organización y para el manejo de datos institucionales, por lo que se

reforzará en la Guía de ciberseguridad estos temas y en próximas acciones que ambas dependencias desean implementar.
Para el diagnóstico se desarrolló un instrumento de consulta masiva, dirigido exclusivamente a las personas teletrabajadoras de la UNED. La encuesta estuvo habilitada del 9 al 15 de noviembre del año 2020 y se elaboró con la aplicación Limesurvey (LimeSurvey 2020). Esta encuesta contó con 65 preguntas, todas de respuesta cerrada.

Se tuvo la participación de 184 personas. Los datos obtenidos fueron exportados de la aplicación de Limesurvey al programa estadístico IBM SPSS Statisctics versión 20 (IBM 2020) para generar la base de datos para el análisis descriptivo, posteriormente se obtuvieron las frecuencias de respuesta y estas se exportaron al programa Microsoft Excel para su respectivo análisis.

II. Perfil de las personas teletrabajadoras de la UNED

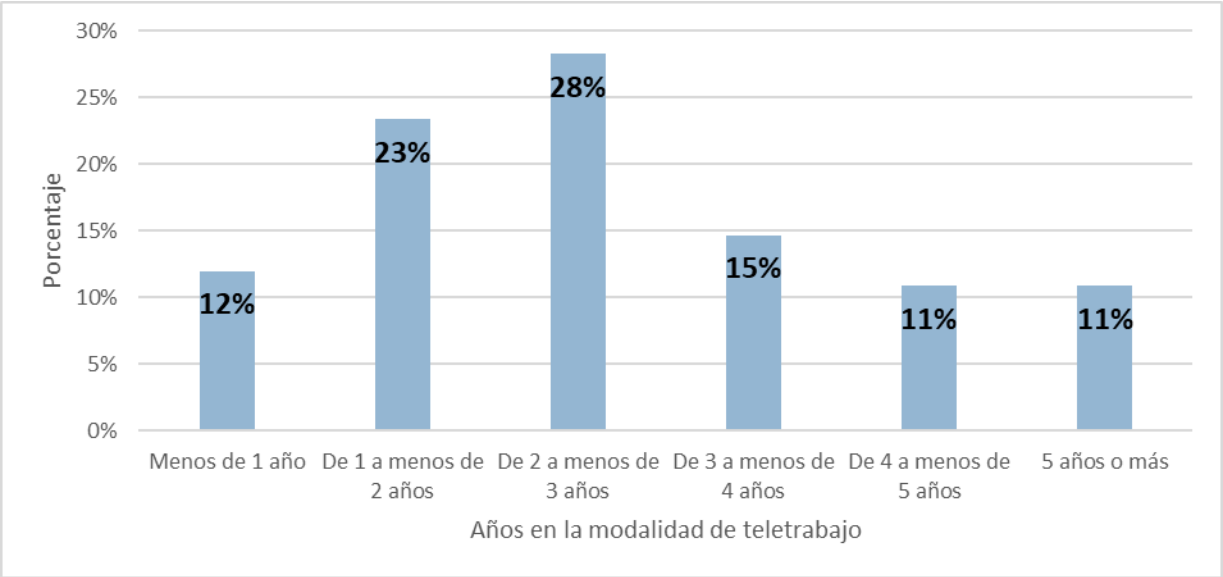
A noviembre del 2020, la UNED contaba con 355 personas teletrabajadoras. No obstante, el diagnóstico fue contestado solo por el 52% de esa población. De las 184 personas que contestaron, el 73% fueron mujeres y el 27% hombres.

El rango de edad de esta población se encuentra entre los 31 y 60 años de edad. Y la mayoría reside en la provincia de San José, y en menor escala en Heredia, Cartago y Alajuela.

Con respecto a su permanencia en la Universidad, el 50% tiene entre 11 y 20 años de laborar para la UNED. Y el mayor porcentaje (59%) labora en la Vicerrectoría Académica, especialmente de las Escuelas y de la Dirección de Producción de Materiales Didácticos.

Y su vinculación con la modalidad de teletrabajo se encuentra principalmente entre 1 y 3 años de ser una persona teletrabajadora. La gran mayoría (82%) realiza teletrabajo domiciliar.

Gráfico 1. Porcentaje de distribución de teletrabajadores de la UNED según los años de pertenecer a la modalidad de teletrabajo



Fuente: Estudio de percepción de la comunidad universitaria de la UNED, 2020.

III. Descripción del equipo tecnológico

El Reglamento de Teletrabajo de la UNED establece en su artículo 16, inciso h) que una persona que desea optar por la modalidad de teletrabajo deberá:

> "Contar con el equipo tecnológico propio, así como la conectividad y accesibilidad indispensables según criterio técnico de la DTIC. En casos debidamente justificados y a solicitud del funcionario, la Administración valorará la posibilidad de dotar al funcionario del equipo tecnológico necesario para teletrabajar".

Por esta razón, el 76% de los encuestados indicaron que el equipo que utiliza para teletrabajar es propio, mientras que el resto manifiesta que teletrabaja con equipo institucional o bien hace una combinación de ambos.

Una consulta que, para efectos del tema de ciberseguridad es muy importante, fue que si el equipo tecnológico propio con el que teletrabaja es compartido con otras personas, y al respecto el 86% indicó que no; sin embargo, el 14% indicó que sí.

Con relación al sistema operativo que utilizan, se divide principalmente entre dos: Windows y el IOs de Macintosh; no obstante, gana por mucho el sistema de Windows.

De ellos el 95% indicó que mantiene actualizado su sistema operativo, pero el 5% indicó que no. De igual manera contestaron ante la consulta de si mantienen los softwares actualizados y el mismo porcentaje, un 5% contestó que no.

Ante la consulta de si utiliza algún software o aplicación sin licencia (que no sea software libre o tenga licencia pública general (GPL) en los dispositivos tecnológicos que utiliza para teletrabajo y para acceder información de la UNED, el 27% contestó que sí.

Sobre el navegador que la mayoría utiliza se concentra en Google Chrome y en menor medida Mozilla Firefox.

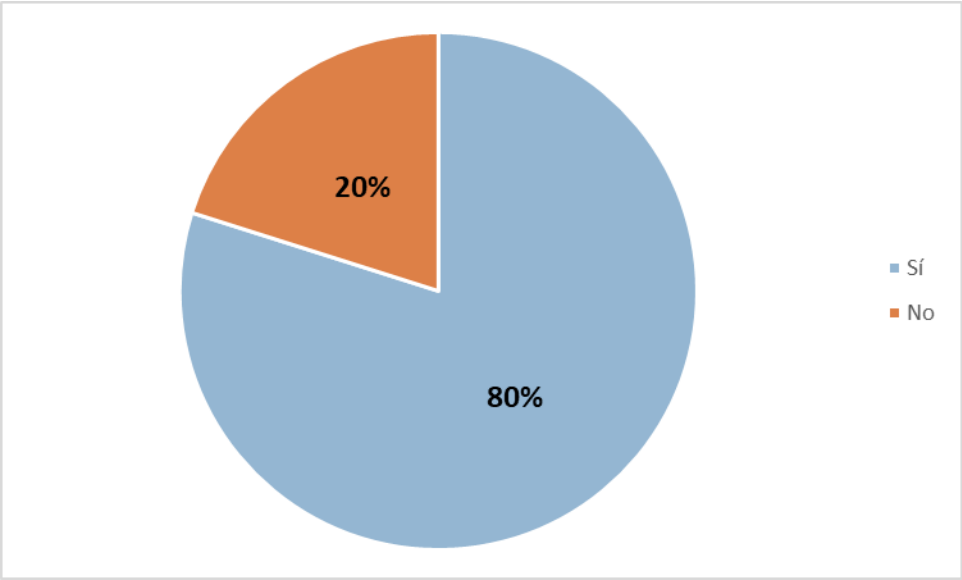
Un firewall o bien, cortafuegos, tiene como propósito bloquear el acceso a otras personas y usuarios a la red privada, o bien a ataques en otras redes. Esto ayuda a prevenir y proteger los datos y el equipo tecnológico que se está utilizando.

Entre los encuestados, se les consultó si utiliza algún software de protección denominado firewall o muro de fuego en su computadora, el 50% respondió que sí, el 19% que no, y el 31% indicó que no lo sabe.

Respecto a los antivirus, se consultaron varios aspectos, y de ello se puede concluir que:

- El 80% sí tiene instalado algún antivirus, pero el otro 20% no.
- El antivirus que utilizan es, en su mayoría, de licencia (47%) y un 33% utiliza un antivirus gratuito.
- Los antivirus más utilizados son el Avast, ESET y el McAfee.
- Solo el 63% afirmó que utiliza el antivirus instalado para realizar revisiones o escaneos periódicos de seguridad en el equipo tecnológico que utiliza para teletrabajar. Dentro de lo que se analiza con el antivirus se encuentran: archivos recibidos por correo electrónico o almacenados en One Drive y Share Point, los archivos que descargan de internet, dispositivos externos como discos duros o USB.

Gráfico 2. Porcentaje de teletrabajadores de la UNED que tienen instalado un antivirus en sus equipos tecnológicos



Fuente: Estudio de percepción de la comunidad universitaria de la UNED, 2020.

Al consultar si se utilizan otros dispositivos para teletrabajar, se les consultó si en la tableta, teléfono o cualquier otro dispositivo móvil utilizan antivirus, solamente el 33% indicó que sí. Por lo tanto, el 67% no utiliza antivirus en otros dispositivos desde los cuales ingresan información de su trabajo.

Una situación similar se da cuando se les consulta si utilizan algún otro software o aplicación de seguridad para proteger y asegurar los dispositivos tecnológicos que utiliza para teletrabajar, pues el 94% indicó que no.

Con respecto a los correos electrónicos que recibe, se les consultó si verifican los siguientes aspectos –los porcentajes brindados son de las personas que indicaron que sí lo verifican-:

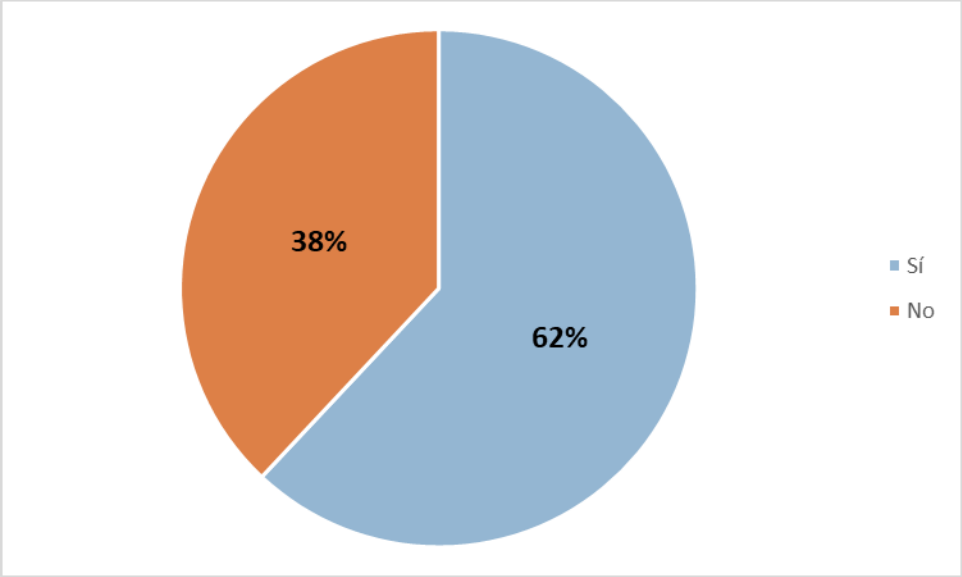
- El remitente del correo es conocido (95%)
- El formato del correo (cuenta@dominio) es conocido y coincide con el recibido en otras ocasiones (75%)
- Revisa el link o url del sitio web antes de darle clic (51%)
- Ninguna de las anteriores (2%)

Y finalmente al consultar sobre la Red Privada Virtual (VPN) o bien el Acceso Remoto VPN se logró recibir los siguientes resultados:

- El 72% sí tiene conocimiento de que es una VPN, pero el 28% no.

- El 62% sí utiliza una VPN, y el 38% no. De ese porcentaje de teletrabajadores que utiliza la VPN que le proporciona la UNED, el 89% la utiliza para acceder a software o aplicaciones institucionales. Y el 57% indicó que sí utiliza la VPN para conectarse a equipos tecnológicos que se encuentran físicamente en la UNED.
- El 67% indica que no tiene conocimientos sobre las medidas de seguridad de una VPN, versus el 33% que indica que si los tiene.

Gráfico 3. Porcentaje de teletrabajadores de la UNED que utilizan VPN



Fuente: Estudio de percepción de la comunidad universitaria de la UNED, 2020.

IV. Manejo de contraseñas y uso del correo electrónico

De acuerdo con el Instituto Nacional de Ciberseguridad “los ciberdelincuentes se sirven de diversas técnicas y herramientas con las que atacar a nuestras credenciales. Los usuarios no siempre les dificultan esta tarea, y suelen caer en malas prácticas que ponen en peligro la seguridad, entre estas malas prácticas se encuentra:

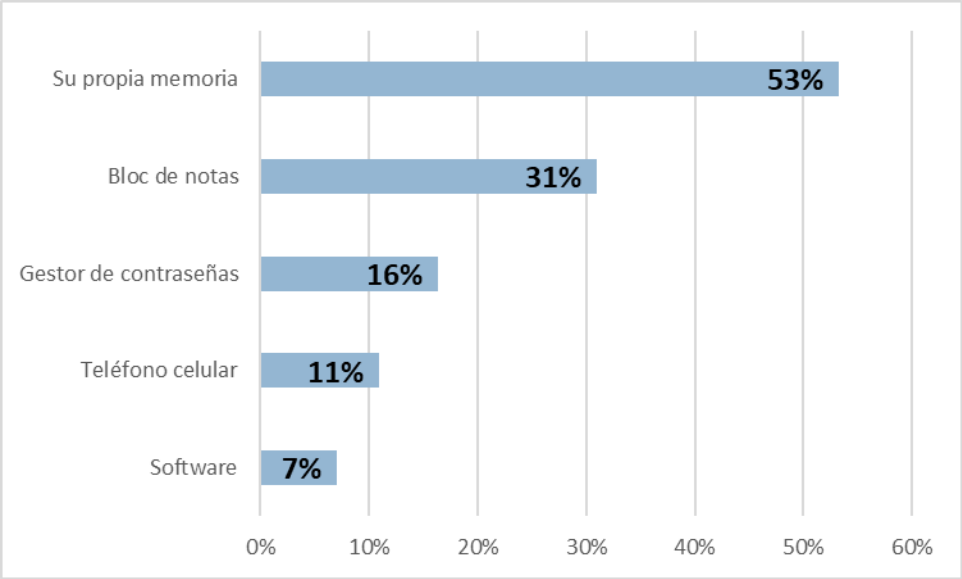
- Utilizar la misma contraseña para distintos servicios.
- Utilizar contraseñas débiles, fáciles de recordar y de atacar
- Utilizar información personal a modo de contraseñas, como la fecha de nacimiento.
- Apuntarlas en notas o archivos sin cifrar.
- Guardar las contraseñas en webs o en el navegador.

- Y finalmente, hacer uso de patrones sencillos, como utilizar la primera letra en mayúscula, seguida de 4 o 5 en minúscula y añadir 1 o 2 números o un carácter especial. Estos patrones acaban por popularizarse, facilitando aún más la tarea a los ciberdelincuentes". (INCIBE, Guía de ciberataques, 2020)

Es por ello por lo que, en este diagnóstico se les consultó a las personas teletrabajadoras de la UNED sobre el manejo de sus contraseñas y al uso del correo electrónico. Al respecto indicaron que:

- Los medios o forma que utiliza para almacenar las contraseñas en su gran mayoría son: su memoria, un bloc de notas, con un gestor de contraseñas y anotándolo en el teléfono celular.
- El 88% afirma que no utiliza una única contraseña para todas las aplicaciones y equipos tecnológicos.
- Asimismo, un alto porcentaje (93%) confirma que no utiliza la contraseña del correo de la UNED como contraseña para acceder a otras aplicaciones no institucionales. Del 7% que indicó que sí utiliza la misma contraseña, agrega que la usa en aplicaciones como Twitter, Gmail, Instagram, entre otras.
- El 91% confirma que no utiliza la cuenta del correo electrónico de la UNED para acceder o validarse en otras aplicaciones no institucionales, no obstante, el 9% indica que sí. De estos últimos, señalan que la han utilizado para validarse o accesar a Facebook, Linkedin, Adobe, entre otros.

Gráfico 4. Porcentaje de los principales medios de almacenaje de contraseñas que utilizan los teletrabajadores de la UNED



1/ Pregunta de respuesta múltiple
Fuente: Diagnóstico sobre ciberseguridad entre teletrabajadores de la UNED, 2020.

Asimismo, se consultó si utilizan la opción de “permitir guardar contraseñas” de páginas y formularios web que brinda los diferentes navegadores web como: Google Chrome, Mozilla Firefox, entre otros. El 37% indicó que sí, mientras que el 63% señaló que no.

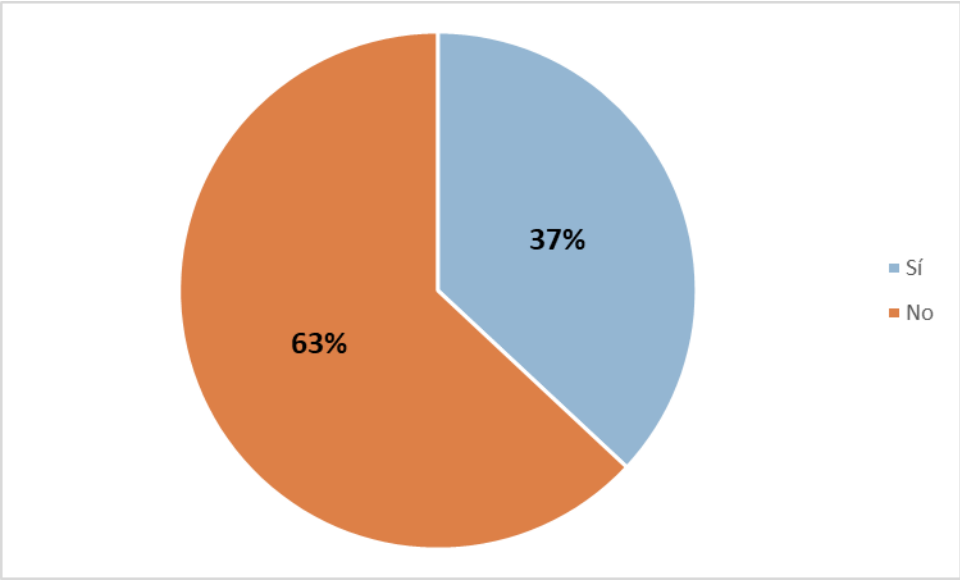
Sobre si cambian con frecuencia las contraseñas de acceso a las aplicaciones institucionales el 67% afirma que sí, no obstante, el 33% indica que no. Quienes contestaron que sí las cambian, explican que lo hacen, en su mayoría cada 90 días, otros cada 60 días y en menor medida cada 30 días o menos.

En materia de ciberseguridad, y específicamente en lo que respecta a las contraseñas, se ha ido evolucionando para brindar mayor seguridad al usuario. Es así como surge lo que se conoce como doble factor de autenticación. INCIBE explica que “en la autenticación de doble factor, el primer factor suele ser la contraseña y el segundo un código aleatorio generado por un *token*, un dispositivo externo, o por una app en el móvil o en el ordenador que en ambos casos posee el usuario”. (INCIBE, 2020)

Con respecto al tema de doble factor de autenticación, el 69% de las personas que contestaron la encuesta, no saben qué es un doble factor de autenticación, y solamente el 31% sí conoce del término. De los que sí comprenden qué es, el 53% indicó que sí lo utiliza, e indicaron que lo acceden con un mensaje de texto, correo electrónico o algún software.

Finalmente, una pregunta de suma importancia para este diagnóstico fue conocer qué hacen las personas cuando reciben correos electrónicos de personas desconocidas. Al respecto, se debe resaltar que un alto porcentaje (83%) indicó que los borra sin abrirlos; no obstante, un 17% los abre y revisa su contenido, un 11% notifica al servicio de apoyo técnico de la DTIC y en un porcentaje menor indica que le pregunta a otra persona si debe abrirlo.

Gráfico 5. Porcentaje de teletrabajadores de la UNED que permite guardar contraseñas a los buscadores



Fuente: Diagnóstico sobre ciberseguridad entre teletrabajadores de la UNED, 2020.

V. Ciberseguridad

Como se indica al inicio, el concepto de ciberseguridad se extiende a todas las buenas prácticas que una persona o una organización implementan para mantener segura su conexión y su información.

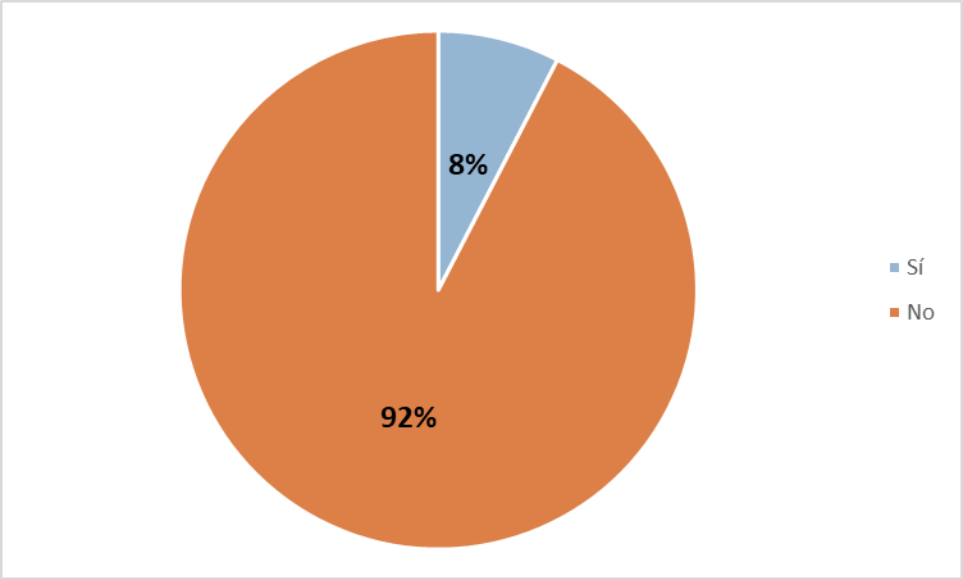
La mayoría de las personas que respondieron el cuestionario, manifestaron conocer los conceptos de: seguridad de la información, seguridad informática, ciberseguridad y buenas prácticas de seguridad digital. No obstante, el 68% manifestó que no ha participado de charlas de ciberseguridad o charlas sobre Seguridad de la Información. Y el 71% indica que la UNED no ha brindado ningún tipo de capacitación, taller o charla asociada al tema de ciberseguridad, seguridad informática o seguridad de la información.

Hay diversos tipos de ciberataques a los que cualquier empresa o persona se puede ver expuesta. Es así como existen ataques: a contraseñas, a las conexiones y por malware.

Las personas que participaron de este diagnóstico indicaron que han recibido llamadas fraudulentas (60%), otros han recibido correos electrónicos relacionados a estafas (42%) y otros en menor escala ha recibido mensajes a su celular con algún matiz fraudulento (21%).

De la totalidad de las personas que contestaron la encuesta, 14 (8%) han sido víctimas de estafa.

Gráfico 6. Porcentaje de teletrabajadores de la UNED que han sido víctimas de alguna estafa mediante medios electrónicos



Fuente: Diagnóstico sobre ciberseguridad entre teletrabajadores de la UNED, 2020.

Con respecto al criterio sobre ¿qué tan seguro consideran que es compartir información privada como nombre, dirección o teléfono en Internet? La mayoría respondió que es muy peligroso o peligroso; sin embargo, poco más del 20% respondió que es más o menos seguro o poco peligroso.

VI. Uso y respaldo de la información

Cuando una persona teletrabajadora requiere acceder a los datos e información institucional va a requerir ingresar a los servidores, ya sean físicos o al almacenamiento en la nube.

Para cualquier organización que implemente la modalidad de teletrabajo es necesario definir cómo se va a acceder a la información y desde cuál equipo tecnológico.

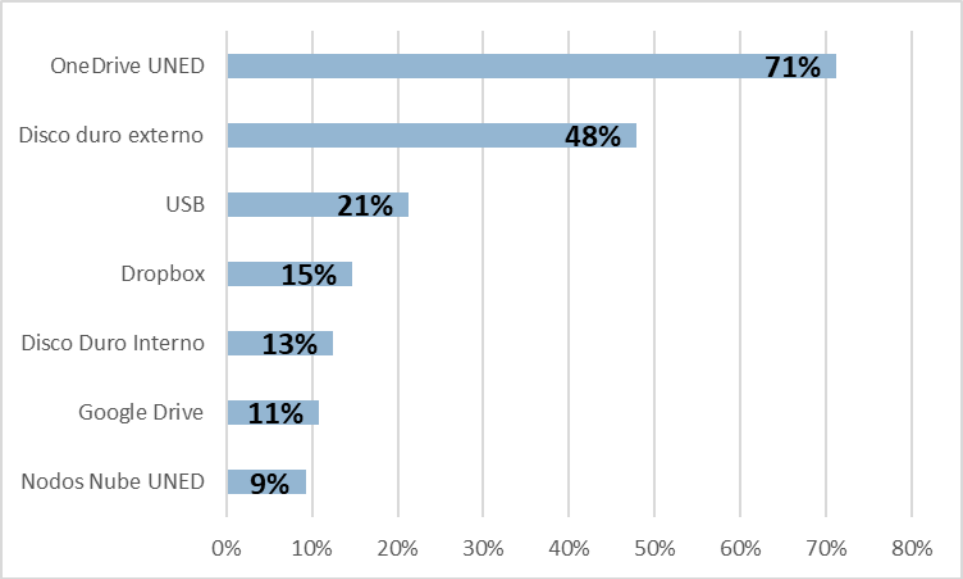
“Para el teletrabajador es muy importante tener acceso a los recursos y datos de la compañía de forma confiable y consistente. Adicionalmente, las soluciones tecnológicas para el teletrabajo deben soportar una gran variedad de necesidades y perfiles, considerando las diferencias entre los grados de habilidad y conocimiento en el área de

conectividad de cada trabajador, lo que obliga a que los procedimientos y dispositivos que permiten el acceso al ambiente corporativo sean simples y muy bien definidos, permitiendo un intercambio fluido y constante de datos". (Colombia, 2020)

En el caso de los teletrabajadores de la UNED que participaron de este diagnóstico se obtienen los siguientes resultados:

- El 85% confirma que respalda la información que contiene en todos sus equipos tecnológicos. El 15% indica que no.
- En cuanto a realizar respaldos de la información institucional que se encuentra en equipos tecnológicos que utiliza para teletrabajo, el 90% afirma que sí lo realiza, pero el 10% que no.
- La gran mayoría realiza sus respaldos en: el OneDrive de la UNED (71%), en un disco duro (48%), en una USB (21%), en Dropbox (15%), Disco duro interno (12%) y en Google Drive (11%).
- El 58% indica que no utiliza el espacio de almacenamiento en la nube de la UNED y el resto (42%) manifiesta que sí lo utiliza.
- Al consultarles si conocen el almacenamiento personal en la nube llamado Microsoft OneDrive que forma parte de la Suite Microsoft Office 365 que utiliza la UNED, el 90% respondió afirmativamente y el 10% restante indicó que no.

Gráfico 7. Porcentaje de distribución de los lugares donde el teletrabajador de la UNED realiza respaldos



Fuente: Diagnóstico sobre ciberseguridad entre teletrabajadores de la UNED, 2020.

VII. Uso del internet

Finalmente, una persona no podría teletrabajar si no cuenta con una conexión a internet. De hecho, esto es una característica fundamental de la modalidad; sin embargo, para el tema de análisis, la seguridad de la información podría verse amenazada según la red desde la cual se conecta la persona teletrabajadora, las claves que utiliza y ciertas prácticas que realice con su equipo tecnológico.

Un aspecto fundamental para conocer más detalles sobre la red y las prácticas que se realizan fue consultar qué tipo de red utilizan. Al respecto el 95% indicó que utilizan una red privada; sin embargo, el resto manifestó que utilizan red pública o desconocen cuál utilizan.

Cuando se conectan a la red, el 75% indica que se le solicita una contraseña; no obstante, el 25% ingresa de manera directa, sin digitar alguna contraseña.

El INCIBE afirma, con respecto a las redes, que “las organizaciones no tienen control sobre las redes que usan sus empleados para teletrabajar. Es una práctica habitual utilizar redes abiertas e inseguras (aeropuertos, cafeterías, etc.) que un ciberdelincuente podría aprovechar para acceder a la información que contiene el dispositivo utilizado para el trabajo en remoto”. (INCIBE, 2020)

El tipo de conexión que utiliza la mayoría de los teletrabajadores (88%) es por medio de wifi o inalámbrica, pero también el 37% indicó que utilizan la conexión por medio de cable ethernet (cable para interconectar dispositivos).

Asimismo, los mecanismos que utilizan para acceder a la información que requieren para trabajar cada día son: One Drive (73%), con un disco duro externo (30%), por medio de una VPN (28%), con un USB (16%), por Google Drive (15%), por Dropbox (14%) y en mucho menor medida, algunas personas indicaron que desde el correo electrónico.

Al encender la computadora o equipo tecnológico, mencionan como primeras actividades que realizan: revisar el correo electrónico (92%), conectarse a una red social el 2%, y el resto de personas en menor porcentaje indicaron que se conectan a la VPN, navegan en la red o hacen respaldos.

Se les consultó también si alguna vez han dado información personal (dirección, número de cédula, contraseña, número de cuentas) a sus contactos de la red y el 60% indicó que nunca; no obstante, el 26% respondió que casi nunca, el 12% que algunas veces y el 2% que muchas veces.

Algunas prácticas que podrían poner en riesgo la información de la organización o el ingreso de ciberdelincuentes, es el participar en rifas, cadenas o concursos en la red. De acuerdo a las respuestas obtenidas en el cuestionario, el 84% indicó que nunca participa, un 10% que casi nunca, y el resto que algunas veces o muchas veces participa en este tipo de actividades.

Como prácticas habituales cuando se utiliza internet, los teletrabajadores señalan casi en la totalidad (99%) el acceso al correo electrónico, la participación en reuniones virtuales (94%), actividades de educación o investigación (82%) y mensajería instantánea (53%). En menores porcentajes se indica que la red la utilizan también para juegos en línea, compras, cursos y escuchar música.

VIII. Reflexiones finales

Este diagnóstico le permitió a la Dirección de Tecnología de Información y Comunicación y al Programa de Teletrabajo conocer con más precisión donde podrían estar las principales vulnerabilidades que pueden afectar a la red, información y equipo institucional.

Aunque en la mayoría de las interrogantes se recibieron resultados satisfactorios, es importante destacar algunos porcentajes, que, aunque no son tan altos, existen, y al existir abren un portillo para que los ciberdelincuentes puedan afectar a la Universidad.

A pesar de que el diagnóstico fue contestado por apenas un 51% de la población teletrabajadora, es un porcentaje significativo que representa las principales prácticas que tienen los teletrabajadores de la UNED. Por lo tanto, para una próxima Guía de ciberseguridad de la UNED es importante considerar que:

1. El 13% indicó que comparte su equipo tecnológico con otras personas en el lugar del teletrabajo.
2. El 5% indicó que no mantiene actualizado su sistema operativo ni los softwares.
3. Falta conocimiento en el concepto y, por ende, en el uso de Firewall.
4. El 20% no tiene instalado un antivirus. Y de las personas que sí tienen instalado un antivirus el 33% indicó que cuentan con un antivirus gratuito.
5. También con respecto a los antivirus, el 67% de las personas confirmaron que no utilizan antivirus en otros dispositivos desde los cuales ingresan información de su trabajo (por ejemplo, tabletas o celulares)
6. El 94% indicó que no utilizan algún software o aplicación de seguridad para proteger y asegurar los dispositivos tecnológicos que utiliza para teletrabajar,

7. Hay un porcentaje significativo que desconoce qué es una VPN y otro que del todo no utiliza VPN. Y el 65% de los que sí la utilizan, informan que no tienen conocimientos sobre las medidas de seguridad de una VPN.
8. Con relación a las contraseñas, un porcentaje muy alto indica que la forma en la que almacena las contraseñas son: su memoria, un bloc de notas, en el teléfono celular. A penas un 16% utiliza un gestor de contraseñas, siendo este la mejor opción para el resguardo de contraseñas.
9. El 9% afirma que sí utiliza la misma cuenta de correo electrónico de la UNED para acceder o validarse a otras aplicaciones como Facebook, LinkedIn, Adobe, entre otros.
10. Además, el 37% confirmó que sí le ha permitido guardar contraseñas a páginas o formularios de la web desde diferentes navegadores.
11. El 33% indica que no tiene como hábito cambiar con frecuencia las contraseñas de acceso a las aplicaciones institucionales.
12. Un tema importante para evitar que los ciberdelincuentes ingresen a información institucional, es contar con un doble factor de autenticación. Lamentablemente la gran mayoría (69%) manifestó desconocer el concepto. Y de los que indicaron que sí comprenden qué es, solo el 17% afirmó que lo utiliza.
13. En relación al uso de correos electrónicos, el 17% manifestó que abre y revisa los contenidos de los correos, aunque provengan de personas desconocidas.
14. Capacitar en materia de ciberseguridad es urgente, puesto que el 71% de las personas que respondieron la encuesta indica que la UNED no le ha brindado ningún tipo de capacitación sobre este tema.
15. Muchas personas indicaron que han recibido llamadas fraudulentas (60%), otros han recibido correos electrónicos relacionados a estafas (42%) y otros en menor escala ha recibido mensajes a su celular con algún matiz fraudulento (21%). Lamentablemente, 14 personas han sido víctimas de estafa.
16. Un 20% de las personas aseguran que compartir información privada como nombre, dirección o teléfono en Internet es más o menos seguro o poco peligroso.
17. En cuanto al respaldo de la información que utilizan para teletrabajar, el 15% indica que no realiza respaldos. El 58% indica que no utiliza el espacio de almacenamiento de la Nube de la UNED, a pesar de que el 90% afirma que sí conocen de la existencia del espacio en Microsoft One Drive.
18. Respecto a la red a la que se conectan, el 25% indica que ingresan de manera directa, sin digitar alguna contraseña. La gran mayoría (88%) confirma que su conexión es inalámbrica.
19. Algunos de los mecanismos que utilizan para accesar a la información institucional son un USB, el cual podría ser fácilmente extraviado, también

utilizan el Google Drive y el Dropbox, que son sistemas de almacenamiento gratuitos.

20. Al conocer si alguna vez han dado información personal (dirección, número de cédula, contraseña, número de cuentas) a sus contactos de la red, el 26% respondió que casi nunca, el 12% que algunas veces y el 2% que muchas veces.
21. Algunas personas, muy pocas en realidad, tienen algunas prácticas cuando ingresan a internet desde sus computadoras, como participar en rifas, cadenas o concursos en la red, así como jugar en línea, realizar compras, cursos en línea o bien escuchar música.

IX. Bibliografía

Colombia, M. d. (2020). *LIBRO BLANCO: el ABC del teletrabajo* . Obtenido de https://www.teletrabajo.gov.co/622/articles-8228_archivo_pdf_libro_blanco.pdf

INCIBE. (2020). Obtenido de https://www.incibe.es/protege-tu-empresa/blog/dos-mejor-uno-doble-factor-acceder-servicios-criticos

INCIBE. (2020). *Guía de ciberataques.*

Kaspersky. (2020). *¿Qué es la ciberseguridad?* Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

X. Anexos

1. MENSAJE ENVIADO A PERSONAS TELETRABAJADORAS DE LA UNED

Estimadas compañeras y compañeros teletrabajadores UNED:

La Dirección de Tecnología, Información y Comunicación (DTIC) y **el Programa de Teletrabajo (PT)** están trabajando en una propuesta institucional sobre **Ciberseguridad para la UNED**, con el objetivo de garantizar conexiones seguras, proteger los dispositivos que se utilizan para trabajar y del adecuado uso de la nube y de toda la información institucional que se resguarda en ella. Además de disminuir los posibles ataques y daños que terceros desean realizar, tanto en equipo e información institucional como en la que ustedes habitualmente utilizan en sus casas.

Para ello, requerimos conocer sobre algunas prácticas que se realizan actualmente por parte de los funcionarios UNED y específicamente de las personas teletrabajadoras. Sabemos que ustedes siempre han sido muy colaboradores al responder las encuestas y los formularios que les enviamos, pero esta vez les SOLICITAMOS A TODOS por favor responder este formulario, ya que nos dará insumos muy valiosos para diagnosticar cómo estamos en ciberseguridad y qué medidas debemos poner en práctica para el bien de todos.

Este formulario les tomará máximo 10 minutos de su tiempo contestarlo, por lo que les pedimos saquen esos minutos para responderlo, de ser posible de una vez y sino máximo al domingo 15 de noviembre. Después de esta fecha se cerrará el formulario.

En caso de tener alguna duda o consulta sobre lo que allí se pregunta, pueden escribirles a los compañeros Alejandro Sánchez Rivera (asanchezr@uned.ac.cr) y Michael González Flores (mgonzalezf@uned.ac.cr) de la DTIC.

Pueden ingresar al formulario dando clic en este enlace:
https://encuestas.uned.ac.cr/index.php/634682?lang=es

Les agradecemos de antemano la colaboración que nos van a brindar al responder este formulario.

Saludos cordiales

2. FORMULARIO ENVIADO A PERSONAS TELETRABAJADORAS DE LA UNED

Consulta sobre Ciberseguridad en el Teletrabajo

Estimadas compañeras y compañeros teletrabajadores UNED:

La Dirección de Tecnología, Información y Comunicación (DTIC) y el Programa de Teletrabajo (PT) están trabajando en una propuesta institucional sobre Ciberseguridad para la UNED.

Para este fin se ha elaborado la presente encuesta, la cual tiene el objetivo de evaluar el conocimiento de ciberseguridad de los teletrabajadores de la Universidad, y de brindar información sobre los aspectos de mejora en el ámbito de seguridad de la información.

De esta manera se busca mejorar en la seguridad de las conexiones, proteger los dispositivos que se utilizan para trabajar y del uso seguro de la nube y de toda la información institucional que se resguarda en ella. Además de disminuir los posibles ataques y daños que terceros desean realizar tanto en equipo e información institucional como en la que ustedes habitualmente utilizan en sus casas.

De manera muy respetuosa le solicitamos completar la siguiente encuesta, toda la información que nos suministre será manejada en estricta confidencialidad y utilizada únicamente para el análisis antes expuesto.

Hay 65 preguntas en la encuesta.

INFORMACIÓN PERSONAL

1. Por favor indique su género.

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Femenino
- ❑ Masculino

2. ¿En cuál rango de edad se encuentra usted?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ De 18 a 30 años
- ❑ De 31 a 40 años
- ❑ De 41 a 50 años
- ❑ De 51 a 60 años
- ❑ 61 años o más

3. Indique la provincia de su residencia.

Por favor seleccione sólo una de las siguientes opciones:

- ❑ San José
- ❑ Alajuela
- ❑ Cartago
- ❑ Heredia
- ❑ Guanacaste
- ❑ Puntarenas
- ❑ Limón

4. Indique el cantón de su residencia.

5. ¿Cuántos años tiene de trabajar en la UNED?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ De 1 a 10 años
- ❑ De 11 a 20 años
- ❑ De 21 a 30 años
- ❑ 31 año o más

6. Indique la instancia superior a la que pertenece la dependencia donde usted trabaja.

_____

7. ¿Cuánto tiempo tiene de estar en la modalidad de Teletrabajo?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Menos de 1 año
- ❑ De 1 a menos de 2 años
- ❑ De 2 a menos de 3 años
- ❑ De 3 a menos de 4 años
- ❑ De 4 a menos de 5 años
- ❑ 5 años o más

8. ¿Qué tipo de teletrabajo realiza?

Por favor seleccione **sólo una** de las siguientes opciones:

- ❑ Domiciliar
- ❑ Móvil

EQUIPO TECNOLÓGICO

9. El equipo tecnológico que utiliza para teletrabajar es:

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Propio
- ❑ Propiedad de la UNED
- ❑ Ambos

10. ¿El equipo tecnológico propio que utiliza para teletrabajar es compartido con otras personas?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

11. Seleccione el sistema operativo de los equipos tecnológicos que utiliza para teletrabajar. (Puede seleccionar más de una opción)

Por favor, marque las opciones que correspondan:

- ❑ Windows 10
- ❑ Windows 8
- ❑ Windows 7
- ❑ Windows XP
- ❑ IOs (Macintosh)
- ❑ Linux
- ❑ No lo sé
- ❑ Otro:

12. ¿Mantiene el sistema operativo o los sistemas operativos actualizados?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

13. ¿Mantiene las aplicaciones y software de sus dispositivos tecnológicos actualizados?
Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

14. ¿Utiliza algún software u aplicación sin licencia (que no sea software libre o tenga licencia pública general (GPL) en los dispositivos tecnológicos que utiliza para teletrabajo y para acceder información de la UNED (por ejemplo: antivirus, programas de diseño, editores de archivos PDF)?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

15. Por lo general ¿cuál navegador web utiliza para visitar páginas web al teletrabajar? *
Por favor seleccione sólo una de las siguientes opciones:

- ❑ Internet Explorer
- ❑ Google Chrome
- ❑ Mozilla Firefox
- ❑ Edge
- ❑ Opera
- ❑ Brave
- ❑ Otro

16. ¿Tiene instalado algún antivirus en el equipo tecnológico que utiliza para teletrabajar?
Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

17. ¿El antivirus utilizado es?
Por favor seleccione sólo una de las siguientes opciones:

- ❑ Licenciado
- ❑ Gratuito

18. ¿Cuál antivirus utiliza?
Por favor seleccione sólo una de las siguientes opciones:

- ❑ ESET (antivirus institucional)
- ❑ ESET (adquirido propio)
- ❑ Avast
- ❑ McAfee
- ❑ Norton
- ❑ Bitdefender
- ❑ Panda
- ❑ Total AV
- ❑ No lo sé

19. ¿Utiliza el antivirus instalado para realizar revisiones o escaneos periódicos de seguridad en el equipo tecnológico que utiliza para teletrabajo?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

20. Utiliza el antivirus instalado en el equipo tecnológico que usa para teletrabajar para realizar revisiones o escaneos de seguridad en:

Por favor, marque las opciones que correspondan:

- ❑ Archivos recibidos por correo electrónico
- ❑ Descarga de archivos de internet
- ❑ Dispositivos Externos (Disco Duro Externo, USB, entre otros.):
- ❑ Disco Duro del equipo tecnológico
- ❑ One Drive
- ❑ Share Point
- ❑ Otro:

21. ¿Utiliza antivirus en su tableta, teléfono o dispositivo móvil?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

22. Cuando usted recibe un correo electrónico verifica lo siguiente:

Por favor, marque las opciones que correspondan:

- ❑ El remitente del correo es conocido.
- ❑ El formato del correo (cuenta@dominio) es conocido y coincide con el recibido en otras ocasiones.
- ❑ Revisa el link o url del sitio web antes de darle clic.
- ❑ Ninguna de las anteriores
- ❑ Otro:

23. ¿Utiliza un software de protección denominado firewall (muro de fuego) en tu ordenador?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No
- ❑ No lo sé

24. ¿Utiliza algún otro software u aplicación de seguridad para proteger y asegurar los dispositivos tecnológicos que utiliza para teletrabajar?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

25. ¿Cuál o cuáles son los otros software u aplicaciones de seguridad que usted utiliza para proteger y asegurar los dispositivos tecnológicos que usa para teletrabajar?

Por favor, escriba su respuesta aquí:

_____

26. ¿Tiene conocimiento de qué es una Red Privada Virtual (VPN) o mejor conocido Acceso Remoto VPN?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

27. ¿Utiliza actualmente alguna VPN?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

28. ¿Tiene algún conocimiento sobre las medidas de seguridad sobre una VPN?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

29. ¿Utiliza la VPN que le proporciona la UNED para acceder a software o aplicaciones institucionales?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

30. ¿Utiliza el acceso remoto VPN que le proporciona la UNED para conectarse a equipos tecnológicos que se encuentran físicamente en la UNED?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

MANEJO DE CONTRASEÑAS Y CUENTA DEL CORREO ELECTRÓNICO UNED

31. ¿Cómo almacena las contraseñas de acceso al correo electrónico institucional, AS400 y demás aplicaciones institucionales?

Por favor, marque las opciones que correspondan:

- ❑ Software
- ❑ Bloc de notas
- ❑ Su propia memoria
- ❑ Teléfono celular
- ❑ Gestor de contraseñas
- ❑ Otro:

32. ¿Suele utilizar una única contraseña para todas las aplicaciones y equipos tecnológicos?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

33. ¿Utiliza la contraseña del correo electrónico de la UNED como contraseña para acceder a otras aplicaciones no institucionales?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

34. ¿En cuáles aplicaciones no institucionales utiliza la misma contraseña que la utilizada en el correo electrónico de la UNED?

Por favor, marque las opciones que correspondan:

- ❑ Facebook
- ❑ Twitter
- ❑ Instagram
- ❑ LinkedIn
- ❑ Gmail
- ❑ Hotmail
- ❑ Otro:

35. ¿Utiliza la cuenta de correo electrónico de la UNED como correo electrónico para acceder y validarse en otras aplicaciones no institucionales?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

36. ¿En cuáles aplicaciones utiliza la cuenta de correo electrónico de la UNED como método de validación, acceso como usuario, cuenta de correo rescate, entre otros?

Por favor, marque las opciones que correspondan:

- ❑ Facebook
- ❑ Twitter
- ❑ Instagram
- ❑ LinkedIn
- ❑ Gmail
- ❑ Hotmail
- ❑ Otro:

37. ¿Utiliza la cuenta de correo electrónico y la contraseña de la UNED como datos para acceder a otras aplicaciones no institucionales?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

38. ¿En cuáles aplicaciones utiliza la cuenta de correo electrónico y contraseña de la UNED?

Por favor, marque las opciones que correspondan:

- ❑ Facebook
- ❑ Twitter
- ❑ Instagram
- ❑ LinkedIn
- ❑ Gmail
- ❑ Hotmail
- ❑ Otro:

39. ¿Utiliza la opción de “permitir guardar contraseñas” de páginas y formularios web que brinda los diferentes navegadores web (como Google Chrome, Mozilla Firefox, entre otros)?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

40. ¿Cambia con frecuencia las contraseñas de acceso a las aplicaciones institucionales?
Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

41. ¿Con qué frecuencia cambia las contraseñas de acceso a las aplicaciones institucionales? *

Por favor seleccione sólo una de las siguientes opciones:

- ❑ 30 días
- ❑ 60 días
- ❑ 90 días
- ❑ Más de 90 días
- ❑ Otro

42. ¿Sabe qué es un doble factor de autentificación?
Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

43. ¿Utiliza el doble factor de autentificación?
Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

44. ¿Cómo accede al doble factor de autentificación?
Por favor seleccione sólo una de las siguientes opciones:

- ❑ Correo electrónico
- ❑ Software
- ❑ Mensaje de texto
- ❑ Llamada telefónica
- ❑ Otro

45. ¿Qué hace cuándo recibe correos electrónicos de personas extrañas?
Por favor, marque las opciones que correspondan:

- ❑ Abrirlos y revisar su contenido
- ❑ Borrarlos sin abrirlos
- ❑ Preguntarle a otra persona si debe abrirlo
- ❑ No uso correo electrónico
- ❑ Notifico al servicio de apoyo técnico de la DTIC
- ❑ Otro:

CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

46. ¿Conoce el concepto de los siguientes términos?
Por favor, marque las opciones que correspondan:

- ❑ Seguridad de la Información
- ❑ Seguridad Informática
- ❑ Ciberseguridad
- ❑ Buenas prácticas de seguridad digital
- ❑ Ninguna de las anteriores

47. ¿Ha participado de charlas de ciberseguridad o charlas sobre Seguridad de la Información?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

48. ¿La UNED le ha brindado algún tipo de capacitación, taller o charla asociada al tema de ciberseguridad, seguridad informática o Seguridad de la Información?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

49. ¿Con relación a las estafas que se han incrementado durante el año, se le ha presentado alguna de las siguientes situaciones?

Por favor, marque las opciones que correspondan:

- ❑ Ha recibido llamadas fraudulentas
- ❑ Ha recibido correos electrónicos
- ❑ Mensajes de Texto SMS
- ❑ Mensajes de WhatsApp
- ❑ Ninguna situación
- ❑ Otro:

50. Considerando lo anterior, ¿usted ha sido víctima de estafa?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

51. ¿Qué tan seguro considera que es compartir su información privada como nombre, dirección o teléfono en Internet?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Muy seguro, no hay problema
- ❑ Más o menos seguro
- ❑ Más o menos peligroso
- ❑ Peligroso
- ❑ Muy peligroso
- ❑ No sé

RESPALDOS DE INFORMACIÓN

52. ¿Respalda la información contenida en todos sus equipos tecnológicos?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

53. ¿Realiza respaldos de la información institucional que se encuentra en el equipo tecnológico que utiliza para teletrabajo?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

54. ¿Dónde realiza dichos respaldos?

Por favor, marque las opciones que correspondan:

- ❑ Disco Duro Externo
- ❑ USB
- ❑ OneDrive UNED
- ❑ Nodos Nube UNED
- ❑ Dropbox
- ❑ Disco Duro Interno
- ❑ Google Drive
- ❑ Otro:

55. ¿Utiliza el espacio de almacenamiento Nodos Nube UNED?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

56. ¿Conoce el almacenamiento personal en la nube llamado Microsoft OneDrive que forma parte de la Suite Microsoft Office 365 que utiliza la UNED?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

USO DE INTERNET

57. ¿Qué tipo de red utiliza para conectarse a Internet?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Pública
- ❑ Privada
- ❑ Otro

58. Cuando se conecta a la red, ¿se le solicita una contraseña?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

59. ¿La red que utiliza para conectarse es compartida por otras personas?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Sí
- ❑ No

60. ¿Qué tipo de conexión de red utiliza?

Marque las opciones que correspondan

Por favor, marque las opciones que correspondan:

- ❑ Wi-Fi
- ❑ Cable ethernet (cable para interconectar dispositivos)
- ❑ Otro:

61. ¿Cómo accede a la información para el trabajo del día a día?

Por favor, marque las opciones que correspondan:

- ❑ Disco duro externo
- ❑ Llave maya
- ❑ One Drive
- ❑ Google Drive
- ❑ Dropbox
- ❑ A través del Acceso Remoto VPN UNED.
- ❑ Otro:

62. ¿Cuál es la primera actividad que realiza al encender una computadora o un dispositivo móvil (teléfono, tableta)?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Conectarse a una red social.
- ❑ Revisar el correo electrónico
- ❑ Navegar en la Red
- ❑ Escuchar o Descargar música
- ❑ Chatear
- ❑ Otro

63. ¿Alguna vez ha dado información personal (dirección, número de cédula, contraseña, número de cuentas) a tus contactos de la red?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Muchas veces
- ❑ Algunas veces
- ❑ Casi Nunca
- ❑ Nunca

64. ¿Participa en rifas, cadenas o concursos de la red?

Por favor seleccione sólo una de las siguientes opciones:

- ❑ Muchas veces
- ❑ Algunas veces
- ❑ Casi Nunca
- ❑ Nunca

65. ¿Qué actividades realiza cuando utiliza internet?

Por favor, marque las opciones que correspondan:

- ❑ Correo electrónico
- ❑ Redes sociales
- ❑ Mensajería instantánea
- ❑ Juegos en línea
- ❑ Reuniones virtuales
- ❑ Series - Películas
- ❑ Educación - Investigación
- ❑ Otro:

Sus respuestas han sido guardadas con éxito.

Le agradecemos mucho la colaboración.