UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL RESISTENCIA

Recomendaciones de Seguridad para la Educación y Trabajo Remoto

GUIA

Primera Edición 2020

Información del documento

Nombre de documento	Recomendaciones de Seguridad para la Educación y Trabajo Remoto		
Preparado por:	Evelin Barrios - Walter Moore - Juan Saenz Kotyk - Carolina Todt	**Versión del documento**:	1.1
Estado del documento:	Pendiente de aprobación		
Revisado por:	Ing. Diego Bolatti - Ing. Andrés Fantin	**Fecha de aprobación**:	29-7-2020

Versión Nro.	Fecha de Versión	Descripción	Revisor	Estado
1.0	22/06/2020	Primera revisión	Ing. Diego Bolatti	Aprobado
1.1	02/07/2020	Segunda revisión	Ing. Andrés Fantin Ing. Diego Bolatti	Aprobado

Tabla de Contenido

Cómo usar esta guía de seguridad

Este documento ha sido preparado como una **guía de seguridad de referencia** para **quienes trabajan y estudian de forma remota**.

Se recomienda a los lectores comenzar por la **sección 1 y 2** para luego abordar la sección de su interés.

Este documento cuenta con 3 **secciones adicionales**, cada una **orientada a un lector en particular**.

La **sección 3** está orientada a **empleados** que realizan trabajo remoto desde su hogar. Dentro de esta sección en la **subsección 3.1** se encuentran **recomendaciones de seguridad** para aquellos empleados que utilizan **dispositivos proporcionados por la empresa** mientras que en la **subsección 3.2** se detallan **aspectos de seguridad** para empleados que **utilizan dispositivos personales**.

La **sección 4** está orientada a los **directivos de una pyme o institución**. Dentro de la cual en la **subsección 4.1** se encuentran **recomendaciones de seguridad para servidores de acceso remoto**. En la **subsección 4.2** se abordan recomendaciones referentes al **control de acceso** que se deben aplicar para los usuarios que deseen ingresar a los sistemas de la institución o empresa. En la **subsección 4.3** se aborda el uso seguro del **correo electrónico**. En la **subsección 4.4** se tratan aspectos referentes a la **administración y resguardo de información sensible**. Mientras que en la **subsección 4.5** se detallan sugerencias para establecer una **comunicación segura entre los miembros de la compañía**. Por último en la **subsección 4.6** se trata la **gestión de incidentes** en el cual se indica cómo habilitar canales de comunicación de emergencias y que procedimientos seguir para reportar un incidente de ciberseguridad.

Mientras que la **sección 5** está orientada a **lectores del ámbito educativo** donde la **subsección 5.1** está dirigida a **estudiantes** y la **subsección 5.2** está orientada a **profesores.**

Por último en la **sección 6** se ofrece un **glosario** con un compendio de **conceptos de seguridad** que se definieron en la guía.

“Todas aquellas palabras que posean un (*) indican que están explicadas en más detalles en el glosario”

1.Introducción

En los últimos años muchas empresas, organizaciones e instituciones educativas han implementado el modo de trabajo y educación a distancia. Esto resulta posible gracias al amplio avance de la tecnología que nos permite realizar nuestras tareas de todos los días desde distintos sitios, pudiendo prescindir de estar presentes físicamente en nuestros lugares de trabajo o estudio.

Sin embargo, esta ventaja viene acompañada de potenciales riesgos a nivel de seguridad informática los cuales deben ser contemplados correctamente. Es importante destacar que actualmente el acceso remoto* con fines laborales y educativos es una oportunidad para el cibercriminal* de causar algún tipo de daño digital.

Según los especialistas, el 99% de los ataques comienza con alguno de los siguientes vectores: el correo electrónico vía phishing* (mediante un engaño haciéndose pasar por otra persona o entidad) o una vulnerabilidad (es decir explotar algún error).

En tal sentido, en este documento ofrecemos una serie de sugerencias y recomendaciones a implementar de manera integral a los fines de aprovechar al máximo la posibilidad de trabajar y estudiar a distancia de forma segura.

Los ataques cibernéticos pueden tener como objetivo dañar sistemas, robar información o bloquear servicios.

1.1 Audiencia

Este **documento** está **destinado** principalmente a lectores del tipo **usuario final** (trabajadores de pymes, empresas, estudiantes, docentes) que poseen un **conocimiento básico de los dispositivos** (celulares, tablets, computadoras, etc.) y **aplicaciones de videoconferencia*** (zoom, hangout, meet, etc.) y/o de acceso remoto*.

2.Descripción general del acceso remoto y su seguridad

Cuando una persona dispone de la posibilidad de realizar sus actividades laborales o educativas desde la comodidad de su casa, ya sea por necesidad o por obligación surgen dos conceptos comúnmente llamados, trabajo remoto* y educación a distancia, ambos conceptos requieren para su implementación lo que llamaremos “Acceso Remoto”. El acceso remoto* concede mediante un ecosistema de aplicaciones una conexión desde un lugar distinto a la organización brindando la posibilidad de acceder a la información no

(*) Véase en glosario de términos

pública de la misma. Este tipo de accesos se puede establecer utilizando una variedad de dispositivos, como ser celulares, tablets, notebooks o PC´s.
Este tipo de acceso brinda la posibilidad de realizar las actividades de forma remota que normalmente serían presenciales, es una gran ventaja pero que a su vez, si no es implementada de forma correcta, puede tener muchas vulnerabilidades asociadas a la misma, una tercera persona ajena a la organización con malas intenciones puede intentar hacer uso de esas vulnerabilidades y perjudicar a la persona u organización. Para disminuir la posibilidad de que ocurran este tipo de situaciones existen medidas a tener en cuenta que explicaremos en la sección 3.

2.1 Vulnerabilidades, amenazas y controles de seguridad

Las soluciones de acceso remoto* necesitan cumplir múltiples requisitos de seguridad si se la quiere implementar de forma correcta, estos requisitos se pueden lograr mediante la combinación de características de seguridad integrada en las aplicaciones de videoconferencia* y nube* de archivos (Zoom, Meet, Drive, Filezilla, etc.) y la aplicación de controles de seguridad en los dispositivos (firewalls*, antivirus, contraseñas).

Los objetivos de seguridad más comunes para el acceso remoto* son los siguientes:

- **Confidencialidad:** asegurar que las comunicaciones de acceso remoto* y los datos del usuario almacenados no puedan ser accedidos por partes no autorizadas.
- **Integridad:** detectar cualquier cambio intencional o no intencional en las comunicaciones de acceso remoto*.
- **Disponibilidad:** asegurar que los usuarios puedan acceder a los recursos a través del acceso remoto* cuando sea necesario.

Para lograr estos objetivos, todos los dispositivos y herramientas de software de acceso remoto* deben ser protegidos contra una variedad de amenazas.

Mientras se esté trabajando desde casa, siempre se debe garantizar la seguridad de los datos y cumplir con las exigencias de seguridad impuestas por la organización y/o entidad, leyes gubernamentales.

Las principales amenazas de seguridad que se presentan en el acceso remoto* son las siguientes:

- **Dispositivos desactualizados:** La mayoría de los dispositivos que se utilizan para el acceso remoto* no tienen actualizado el sistema operativo* y antivirus.
- **Falta de controles de seguridad física:** Los dispositivos del usuario se utilizan en diferentes ubicaciones como ser en el hogar, cafeterías, hoteles, restaurantes, etc.
  La naturaleza móvil de estos dispositivos los hace más propensos a la pérdida o el robo de los mismos, lo que comprometería los datos o conexiones que posee.

(*) Véase en glosario de términos

- **Redes inseguras:** Como el acceso remoto* requiere del uso de internet el mismo utiliza protocolos, es decir configuraciones y procedimientos estándares conocidos a nivel global, y por esta razón son susceptibles a ataques (por ejemplo man-in-the-middle, entre otros). Para mitigar este tipo de riesgos se pueden utilizar mecanismos de encriptación* y verificación de identidad que dificultan los posibles ataques.
- **Dispositivos comprometidos en redes internas:** Cuando se permite que un usuario se conecte directamente a la red interna utilizando sus propios dispositivos que han estado conectados en redes externas o al alcance de un atacante, se corre el riesgo de infectar la red de la organización. El atacante pudo haber instalado algún Malware* en el dispositivo para recopilar información y transferirsela, este Malware* también se puede propagar a otros dispositivos internos de la organización permitiendo que el ataque prosiga luego de que el dispositivo infectado sea desconectado.

3. Recomendaciones de Seguridad para los empleados

En esta sección se presentan recomendaciones de seguridad para los trabajadores de las empresas Regionales y Pymes. Disponer de un espacio adecuado para trabajar desde el hogar sin riesgo a perder información por causa de daño del equipo por la mala manipulación de alimentos, por ejemplo.

3.1 En caso de utilizar dispositivos electrónicos proporcionados por la Empresa

3.1.1 Conectividad

- **Siempre utilizar conexiones VPN (Red Privada Virtual)*:** te permite el acceso seguro a la red de la empresa utilizando la conexión a Internet de tu casa. Esto evita que el tráfico sea interceptado por un ciberatacante.
- **Evitar conectarse a Wi-Fi de espacios públicos** como el de un bar o espacio social.
- **Verificar el Wi-Fi hogareño:** controlá que tu router posea una contraseña WPA2 y cámbiala regularmente.

(*) Véase en glosario de términos

- **Reforzar la seguridad de las comunicaciones.** En la medida de lo posible, conviene siempre acceder a páginas “https” (de conexión segura) y utilizar una autenticación de doble factor* en las comunicaciones.

Es importante tener en cuenta que todo dispositivo que se conecte a internet es vulnerable a sufrir una infección por malware.

3.1.2 Contraseñas y configuraciones de seguridad:

- **Configurar una contraseña o activar datos biométricos para acceder al dispositivo.** Este último siempre se debe bloquear cuando no estemos trabajando en él.
- **Cambiá tus contraseñas regularmente** y jamás las compartas con nadie. Recordemos que para que sea robusta debe contener como mínimo 8 caracteres, una mayúscula, un número y un carácter especial con la finalidad de cumplir con el respaldo de una contraseña segura*. Es fundamental que no utilices la misma contraseña para todos las cuentas/ perfiles para acotar el riesgo de pérdidas.
- **Activa la Autenticación de Múltiples Factores** en todos los servicios y apps que permitan esta configuración, sobre todo si tenés instaladas aplicaciones con información laboral en tu celular personal.
- Recordá que **la seguridad de tus contraseñas no solo depende de vos,** sino también del sitio donde las ingreses. Muchas veces visitamos sitios que no son seguros y las contraseñas se ven comprometidas. En este sentido, recomendamos verificar que la dirección URL* del sitio al que queramos acceder esté bien escrita y que comience con HTTPS. Además, chequear que el certificado SSL* del sitio esté expendido a quien corresponda, esto lo podés ver haciendo click en el candadito que aparece en la barra de navegación.

Las contraseñas deben ser:

- **Personales**
- **Intransferibles**
- **Modificadas sólo por el dueño**
- **Secretas**

3.1.3 Correo electrónico

- **Prestá atención respecto a correos electrónicos fraudulentos**, es decir campañas de phishing*. A través de estos podríamos infectar el equipo con un malware* o generar una fuga de información. Recordá no hacer click en enlaces ni

(*) Véase en glosario de términos

descargar archivos adjuntos* que provengan de un remitente desconocido o sospechoso.

- **Utiliza el mail institucional,** sobre todo para realizar intercambios de archivos oficiales. Si no posees una cuenta, recomendamos que la solicites cuanto antes al sector correspondiente.
- **No enviar información sensible.**
- **Utilizar la opción de copia oculta.**
- **Ser prudente a la hora de contestar los correos.**
- **No reenviar correos de orígenes desconocidos.**
- **Cifrar los correos importantes.**

En un mundo cada vez más hiperconectado, es muy importante tener presente que la seguridad digital es un asunto de todos por igual y empieza por cada uno de nosotros.

3.1.4 Seguridad de la información

- Siempre que sea posible **trabajá los archivos desde la Nube**, es decir, no los descargues localmente a tu dispositivo para editarlos. La mayoría de los servicios de este tipo cuentan con editores online.
- Asegurate de **sincronizar bien todos los archivos** para así evitar pérdidas de información.
- **No almacenar información sensible y/o confidencial en pendrives o discos extraíbles* personales.**
- Si necesitás **compartir un archivo o documento confidencial podés encriptarlo** para enviarlo por correo electrónico y hacerle llegar al destinatario la contraseña por otro medio o plataforma*.
- **No enviar archivos con información de la organización y/o entidad, por medios no oficiales** como whatsapp, dropbox, wetransfer, correos de dominio gratuito, etc.

3.1.5 Seguridad en los navegadores web

- **Mantener actualizado el navegador web** que se utilice y sus plugins o extensiones.
- **Elimina todos los plugins que desconozcas** o que no sepas para qué sirven ya que podrían tratarse de algún tipo de malware*.
- **Prestá atención a los gestores de contraseñas** que vienen instalados por defecto en los navegadores para que no guarden datos de inicio de sesión.
- **Evita navegar por páginas sin certificado digital SSL*, te darás cuenta porque carece del https y el navegador web te lo advertirá.**

(*) Véase en glosario de términos

3.1.6 Seguridad en los dispositivos móviles

- **No enviar mensajes de texto con datos confidenciales**, como información privada y detalles de las credenciales de acceso*.
- **Cifrar el dispositivo móvil**, implementar en los dispositivos mecanismos de cifrado de la documentación además de los de autenticación* de usuarios.
- **No conectarse a redes Wi-Fi públicas** abiertas o hotspots.
- **No instalar ninguna aplicación que no provenga de una fuente de confianza**, como las tiendas oficiales de Apps o las proporcionadas de manera oficial por la Organización.
- **Realizar copias de seguridad** periódicas sincronizadas con los servicios de nube*.
- **Mantener actualizado el sistema operativo del celular.**

3.2 En caso de estar utilizando dispositivos electrónicos personales

Si no contamos con la posibilidad de que nuestro empleador nos brinde los dispositivos necesarios para cumplir con nuestras funciones, tendremos que recurrir a los equipos personales que tengamos a disposición.
Además de las medidas anteriormente mencionadas, debemos tener en cuenta las siguientes recomendaciones de seguridad, sobre todo si se trata de dispositivos de uso compartido con otros integrantes del hogar.

- Para los **dispositivos compartidos crear un perfil con usuario y contraseña diferentes,** para el uso laboral.
- Tener la **precaución de borrar datos y documentación confidencial de las carpetas compartidas** que hayas utilizado y de la papelera de reciclaje.
- Si se trata de un dispositivo móvil (celular o tablet), **descargá las aplicaciones** que necesites únicamente de las **tiendas oficiales** de Android o iOS.
- **Evita mezclar tu vida privada con la institucional,** esto quiere decir que mientras estés utilizando el dispositivo evites usar tus redes sociales, correo electrónico personal y homebanking (o similares).
- **Tener instaladas las últimas actualizaciones** del sistema operativo*.
- **Tener actualizados los antivirus** con la mayor frecuencia posible.
- **Intensificar el uso del doble factor de autenticación** en los accesos a sistemas, equipos, etc.

(*) Véase en glosario de términos

4.Recomendaciones para instituciones y empresas pymes.

Se recomienda, en la medida de lo posible, que los empleadores equipen a sus empleados con dispositivos que cumplan con las políticas de seguridad de la información correspondientes a cada institución y sector.
Si esto no es posible y el usuario debe recurrir a utilizar sus dispositivos personales para poder desarrollar sus tareas, lo ideal sería que, en conjunto con el área de sistemas, IT o quien corresponda, verifiquen que dichos dispositivos se encuentren en las correctas condiciones de seguridad: sistema operativo*, antivirus actualizados, etc.
Por otra parte, queremos destacar la importancia de capacitar a todas las personas que forman parte de las instituciones/empresas en materia de ciberseguridad ya que estas acciones pueden reducir hasta en un 90% las probabilidades de sufrir un ataque a nivel corporativo o institucional.

En esta sección se presentan algunas recomendaciones de seguridad para empresas e instituciones.

Dada la alta exposición que se tiene a los virus informáticos, es imprescindible hacer uso de programas antivirus en todos los dispositivos que se utilicen conectados a internet.

4.1 Seguridad del servidor de acceso remoto

La seguridad de los servidores de acceso remoto* son particularmente importante porque proporcionan una vía para que personas externas tengan acceso a recursos internos de la organización.
Algunas recomendaciones de seguridad para los servidores de acceso remoto* son las siguientes:

- **Los servidores de acceso remoto* se deben colocar en un host separado** y dedicado para reducir y limitar el impacto de un posible ataque malicioso.
- **Se debe considerar múltiples soluciones de acceso remoto*** según las necesidades de seguridad de los usuarios. Listas de acceso mediante roles y permisos.
- **Aquellos servidores que almacenan datos confidenciales de los usuarios temporalmente deben ser borrados** una vez que se dejan de utilizar o luego de un periodo de tiempo determinado.
- **Activar los registros de auditorías.**
- **Forzar el uso de doble factor de autenticación* y la complejidad de contraseñas.**
- **Implementar un programa de copias de seguridad que se ajuste a las políticas.**

(*) Véase en glosario de términos

4.2 Autenticación, autorización y control de acceso

4.2.1 Autenticación

Hay muchas maneras de autenticar a usuarios de acceso remoto*, a través de contraseñas, certificados digitales, controles de acceso, monitorización de las redes, o tokens de autenticación*.

Ya que la contraseñas son la única forma de autenticación* en la mayoría de los casos, para accesos remotos se debería **considerar una contraseña que sea distinta a las usadas para su correo electrónico, home banking, redes sociales, cuentas de compras por internet,** etc.

Tener contraseñas diferentes reduce el impacto de la pérdida de información privada o del organismo para el cual trabaja. Si las necesidades de seguridad de la organización para la cual trabaja son mayores, se puede considerar el uso de doble factor de autenticación como mecanismo de refuerzo a la seguridad o la instalación de certificados de seguridad que permitan validar los dispositivos accesibles.

Utilizar contraseñas seguras constituye la primera línea de defensa para la protección de la información.

4.2.2 Autorización

Después de verificar la identidad de un usuario de acceso remoto*, se debe determinar cuales son los recursos internos a los que pueden tener acceso. Para determinar esto el servidor de acceso remoto* puede **realizar comprobaciones del estado del dispositivo del usuario**.

Estas comprobaciones de estado generalmente requieren de un **software en el dispositivo del usuario**, que esté controlado por el servidor de acceso remoto* para **verificar el cumplimiento** de ciertos **requisitos de configuración segura** establecida por la organización, por ejemplo que el software antimalware del usuario esté actualizado, el sistema operativo* está completamente parcheado, que el dispositivo no esté rooteado, etc.

Según los resultados de estos controles, se **permite o no el acceso remoto*** y los **recursos** que se **puede utilizar.**

Si el usuario tiene credenciales de autorización aceptables pero el dispositivo no pasa la comprobación de estado, el usuario y el dispositivo pueden tener acceso limitado a la red interna. Esta decisión puede basarse en la parte de la red a la que el dispositivo está intentando acceder; una organización podría tener políticas más estrictas para datos más confidenciales.

4.2.3 Control de acceso para aplicaciones

Establecer si el usuario necesita acceder a la red interna de la organización/institución o simplemente acceso a servicios y correo electrónico basados en la nube. Como así también considerar otorgar el mismo nivel de acceso a la información confidencial.

(*) Véase en glosario de términos

Si se necesita acceso a la red interna de la organización:

- **Se recomienda hacerlo desde un dispositivo que sea propiedad de la organización/institución** a la cual pertenece, para que el control total del dispositivo que se conecta esté bajo la supervisión del equipo de seguridad y del departamento de tecnología.
- **Utilizar una VPN* para conectarse a la red interna de la organización/institución.**
- **Controle el uso de dispositivos externos**, como los de almacenamiento USB, así como otros dispositivos.

4.3 Correo Electrónico

- **Incentivar la utilización del correo institucional** para el intercambio de archivos. Además, es fundamental hacer hincapié en que los temas oficiales deben ser tratados por canales oficiales.
- **Solicitarles a los empleados la implementación del múltiple factor de autenticación*** mediante una app, sobre todo si la tienen instalada en el celular.
- **Envío y recepción.** Bloquear correos con scripts o ejecutables, macros, listas negras.
- **Activar filtros antispam**, tanto en el servidor como en los clientes de correo electrónico, que impidan el acceso de correo malicioso.

El correo electrónico es la principal amenaza para la ciberseguridad de las empresas.

4.4 Seguridad de la Información

- **Reforzar la política de respaldo de la información sincronizando todos los archivos en la Nube**. Además, incentivar a los empleados a modificar los archivos desde los editores online que poseen estos servicios.
- **Realizar frecuentemente backups fuera de línea** para resguardar información, archivos, documentos y cualquier tipo de activo digital de posibles ataques ransomware*.
- **Evaluar la encriptación* de discos** en equipos institucionales por si estos llegasen a manos equivocadas. De esta manera se asegura que no se pueda acceder a datos sensibles y/o confidenciales.
- **Revisar las políticas de auditoría para evitar inconvenientes en cuanto a los derechos de propiedad** intelectual de documentos desarrollados en equipos personales de los trabajadores.
- **Digitalizar todos los documentos que aún estén en papel** y que se requieran para trabajar remotamente. Si se trata de información sensible o confidencial se recomienda configurar el bloqueo por contraseña para poder visualizarlo.

(*) Véase en glosario de términos

Es fundamental entender que las copias de seguridad de la información es lo único realmente efectivo ante algún daño o pérdida de datos.

4.5 Comunicación

- **Recomendamos establecer canales de comunicación oficiales y ágiles** con el área de soporte para la resolución de problemas técnicos que puedan llegar a tener los usuarios.
- **Implementar una plataforma de videollamadas segura y confiable** para poder realizar reuniones no presenciales.
- **Asegurarse de capacitar y concientizar a todos los empleados** que realicen home office sobre los riesgos relacionados a la seguridad de la información: phishing*, infección por malware*, brechas de seguridad, fuga de información, etc. Como así también fomentar e incentivar las buenas prácticas de seguridad informática.
- Recuerde al **personal** que **lea y conozca las configuraciones básicas de seguridad y privacidad** como:
    - Tener una **contraseña para cada reunión** o llamada de conferencia.
    - La **cámara debe estar apagada** o bloqueada de manera predeterminada, tanto para el anfitrión como para los asistentes.
    - El **micrófono debe estar en silencio** por defecto.
    - Los **participantes eliminados no pueden volver a unirse**.
    - Solicite al personal que se asegure de que sus reuniones **NO se graben**.
    - **Si está grabando, informe** a todos los **participantes**.
    - Recuerde al personal SALIR o **cerrar la aplicación** una vez que se **complete la conferencia**.

Sin conciencia, no hay seguridad.

4.6 Gestión de Incidentes

- **Habilitar un canal de comunicación para emergencias:** si un trabajador llega a detectar un incidente de ciberseguridad durante su jornada laboral en casa es fundamental poder actuar cuanto antes para mitigar los posibles daños.
- **Tener procedimientos claros para actuar ante diferentes escenarios e incidentes** y asegurarse que cada una de las personas que intervengan en dicho procedimiento lo sepan a la perfección.

(*) Véase en glosario de términos

5. Recomendaciones de seguridad para estudiantes y profesores

Actualmente los estudiantes completan sus asignaturas, se comunican con sus compañeros de clases, revisan sus calificaciones y realizan sus investigaciones en línea.

El Internet ha impulsado la habilidad de los estudiantes para aprender y acceder a una cantidad de información infinitamente superior a la que puede contener una biblioteca escolar.

Sin embargo, el mundo cibernético de la educación moderna puede albergar riesgos en los distintos centros educativos, tanto para los estudiantes como para los profesores.

La evaluación debe constituirse como parte de los procesos de enseñanza y aprendizaje más que un simple suceso pedagógico adaptándose a los nuevos métodos de evaluación del nuevo ecosistema de aprendizaje.

A continuación se mencionan recomendaciones de seguridad para los estudiantes y profesores.

5.1 Recomendaciones de seguridad para los estudiantes

- **Mantenga protegido sus dispositivos.** Habilitar el firewall* en los dispositivos, así como software antimalware y antivirus.
- **No ignorar las actualizaciones de seguridad.** Manténgase seguro y actualizado configurando actualizaciones y parches automáticos para software y sistemas operativos.
- **Evitar las aplicaciones riesgosas.** Reduzca el potencial de ataque de su red y dispositivos, elimine cualquier aplicación si no es necesaria.
- **No responder ni dar clic en vínculos cuya fuente no podamos validar**. Fuente de distribución de virus y aplicativos de partes de los delincuentes informáticos.
- **Aplicaciones de proveedores oficiales**. Descarga únicamente aplicaciones de tiendas oficiales intentando mantenerlas actualizadas de manera permanente.
- **Redes seguras**. Establezca permisos de usuario en todos los dispositivos, permitiendo el acceso solo a aquellos que necesitan estar vinculados a la red. Proteja las redes con frases de contraseña y cambie todas las contraseñas predeterminadas en dispositivos de la casa que se conectan a la red. No escriba frases de contraseña para que otros las vean (en una nota adhesiva, por ejemplo), ni las comparta con nadie.
- **Protege tu propia red.** Si tiene muchos visitantes, configure una red de invitados, separada de la que usa para las clases virtuales.

(*) Véase en glosario de términos

- **Nunca use unidades USB aleatorias o encontradas.** Conectar una unidad USB desconocida podría introducir malware* en su dispositivo.
- **Al navegar en las páginas web prestar atención a la presencia del candado.** Indica que la información intercambiada está cifrada mediante algún protocolo de seguridad.
- **Aprenda a evitar las estafas de phishing.** Haga una pausa antes de hacer clic en enlaces en correos electrónicos, mensajes o en sitios de redes sociales. Obtenga una vista previa de los enlaces no reconocidos o sospechosos al pasar el mouse sobre ellos (no avance más si hay errores ortográficos u otras irregularidades, o si el enlace no coincide con el texto). Preste atención a los mensajes con saludos genéricos y archivos adjuntos* con sospecha. Verifique los mensajes por teléfono o en persona si es necesario.
- **Tome precauciones durante el tiempo de inactividad.** No comparta información en exceso en las redes sociales. Los hackers pueden usar datos personales compartidos en línea para cometer fraude.
- **Copias de seguridad.** Realice regularmente copias de seguridad de datos importantes para que, si es víctima de ransomware*, pueda recuperar sus archivos sin tener que pagarlos.
- **Mejorar la seguridad física.** Mantenga las puertas cerradas, utilice candados de anclaje y guarde las computadoras portátiles en cajones cerrados cuando no estén en uso. Descarte los datos confidenciales (en papel, memorias usb, discos duros y otros medios electrónicos) destruyendolos de forma segura.
- **Pedir asesoramiento y ayuda.** En caso de tener problemas de seguridad con sus dispositivos o plataformas* reportarlo al administrador para que pueda ayudarlo y prevenir a toda la comunidad educativa sobre la problemática.

5.2 Recomendaciones de seguridad para profesores

5.2.1 Aula Virtual

- **No publicar los enlaces** de reuniones de las clases en la web.
- **Asegurarse que las contraseñas sean obligatorias** para los estudiantes participantes de las clases virtuales.
- Asegurarse de **verificar la lista de estudiantes al enviar la invitación** a la reunión de la clase.
- **Habilitar la sala de espera** en las clases virtuales.
- Asegurarse de **revisar la lista de participantes** durante la clase virtual.
- Asegurarse que su **aplicación de videoconferencia* esté actualizada** y tenga la opción activada de las actualizaciones automáticas.
- **Separar el área personal del área de trabajo**. Fotos, videos, archivos deben ser almacenados en diferentes carpetas para evitar durante una clase virtual, la difusión por error de información privada.

(*) Véase en glosario de términos

- **Deshabilitar la transferencia de archivos** durante la clase.
- Configurar el **uso compartido de pantalla solo para el anfitrión** de la reunión.
- **Conversar con los estudiantes acerca del cibercrimen.** Necesitan ser tan precavidos como usted. Muchos jóvenes tienen el conocimiento suficiente para darse cuenta de que descargaron un virus, pero pocos se sienten dispuestos a pedir ayuda o admitir el error a sus padres y profesores.

El diálogo con los estudiantes es clave para disminuir los riesgos de seguridad.

5.2.2 Exámenes Online

- Los **estudiantes deben estar registrados y autenticados** para acceder al contenido del examen.
- Se debe pedir a los estudiantes **mostrar el lugar donde están efectuando el proceso evaluativo** dejando encendido en todo momento su cámara web y el micrófono, así como probar su identidad mediante la muestra de su documento nacional de identidad.
- **Definir una clave para acceder al examen**, la cual será válida solo en la franja de horario de inicio y finalización establecidos para la instancia evaluativa.
- Los exámenes orales a través de una **videollamada deben ser grabados**.
- El **examen y sus resultados deben ser almacenado en un lugar seguro** y encriptado.
- Sólo **los estudiantes autorizados pueden acceder a los resultados** de los exámenes.
- **Utilice aplicaciones y herramientas oficiales** autorizadas por la entidad educativa para realizar los exámenes.

5.2.3 Contraseñas

- **Establecer contraseñas complejas**, compuestas por una combinación de mayúsculas y minúsculas e incluir números y símbolos.
- **Cambiar la contraseña periódicamente.**
- **Utilizar diferentes contraseñas** para cada cuenta.
- **Verificar la fortaleza** de tu contraseña.
- Considerar la utilización de **contraseñas biométricas**.
- Utilizar la **autenticación de dos factores**.
- **No usar referencias directas** de las **cosas que publicamos en las redes sociales** como contraseñas.

5.2.4 Correo Electrónicos

- **Prestar atención respecto a correos electrónicos fraudulentos,** es decir campañas de phishing*. A través de estos podríamos infectar el equipo con un malware* o generar una fuga de información. Recordá no hacer click en enlaces ni

(*) Véase en glosario de términos

descargar archivos adjuntos* que provengan de un remitente desconocido o sospechoso.

- **Utilizar el mail del centro educativo,** sobre todo para realizar intercambio de archivos oficiales. Si no posees una cuenta, recomendamos que la solicites cuanto antes al sector correspondiente.
- **Archivos adjuntos extraños.** No deben abrir un archivo adjunto si parece no ser necesario o no estar relacionado con el mensaje, podrían instalar malware* en tu dispositivo.

5.2.5 Dispositivos móviles

- **Mantener actualizado los dispositivos móviles.** Actualizar el sistema operativo*, las aplicaciones y los antivirus del dispositivo.
- **Realizar resguardos periódicos de la información** importante almacenada en el dispositivo móvil.
- Utilizar el **bloqueo de pantalla automático** en los dispositivos.
- En caso de que varias personas utilicen el mismo dispositivo crear **perfiles para cada usuario.**
- **Personalizar la configuración de cifrado.** Si tu dispositivo no tiene por defecto habilitado el cifrado, habilítalo.

(*) Véase en glosario de términos

6. Glosario

Acceso Remoto: Acceder desde un dispositivo a información que se encuentra en un lugar físico distante.
Archivos adjuntos: Son archivos que se envían junto con un correo electrónico.
Ataques cibernéticos: Acciones que intentan exponer, alterar, desestabilizar, destruir, eliminar datos u obtener acceso sin autorización.
Autenticación: Validar que la persona es quien dice ser.
Autenticación de doble factor: Ver *Múltiple Factor de Autenticación.*
Certificado SSL: Es un estándar de seguridad global que permite la transferencia de datos cifrados entre un navegador y un servidor web, se observa la presencia de las siglas “https”.
Cibercriminal: Persona que comete ataques cibernéticos.
Contraseña segura: Incluye características como números, combinaciones de letras mayúsculas y minúsculas, caracteres especiales (- * ? ! @ # $ / () {} = . , ; :) y además posee una longitud mayor a 8 caracteres. La misma debe evitar referenciar de manera directa a datos personales, los cuales son fáciles de obtener por un posible perpetrador, ni utilizar la misma contraseña en distintos lugares. Evitar los patrones numéricos seguidos (123456) o repetición de caracteres (111111). Siempre evite compartirla, anotarla en un papel al alcance de terceros o resguardarla en medios electrónicos como ser el correo.
Credenciales de acceso: Son datos privados que permiten el acceso a determinados sitios digitales restringidos, comúnmente se utilizan usuarios y contraseñas.
Dirección URL: Dirección única que me permite acceso a recursos web.
Discos extraíbles: Unidades de almacenamiento de fácil conexión y transporte.
Encriptación: Método en el que mediante la aplicación de una clave y un algoritmo se cifra una determinada información y solo pueda ser accedida por quien posea dicha clave.
Firewall: Dispositivo de seguridad que monitorea el tráfico de una red permitiendo accesos autorizados y bloqueando los que no lo fueran.
Malware: Es un software malicioso con la intención de dañar dispositivos.
Múltiple Factor de Autenticación: Es un método de control de acceso informático en el que a un usuario se le concede acceso al sistema solo después de que presente dos o más pruebas diferentes de que es quien dice ser.
Navegadores web: Programas que permiten el acceso a la web, es decir a las direcciones URL.
Nube(informática): Nuevo paradigma de prestación de servicios de computación a través de internet.
Phishing: Conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.
Plataforma(informática): Es un sistema que sirve como base para hacer funcionar determinados módulos de hardware o de software con los que es compatible.
Ransomware: Es un programa dañino que restringe el acceso a determinados archivos del dispositivo y pide un restacate monetario a cambio de volverlos a liberar.

Redes Wi-Fi: Redes que permiten el acceso sin cables a la red de un determinado lugar.
Servidores de acceso remoto: Servidores conectados a una red como ser internet que permiten que, bajo determinados criterios, se establezcan conexiones con el mismo para acceder a sus datos.
Sistema operativo: Programa que gobierna los componentes de una computadora y permite al usuario realizar operaciones con la misma.
Trabajo remoto: Acción de realizar las tareas laborales a través de internet desde una ubicación distinta a la ubicación de la institución para la cual se trabaja.
Videoconferencia: Establecer una llamada a través de internet en la cual los participantes pueden establecer contacto mediante voz y video si así lo desean.
VPN (Red Privada Virtual): Una red privada virtual es una tecnología de red de ordenadores que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.

7. Referencias

Exam Security Protocol (2020). Uregina. Recuperado el 16 de Junio de 2020, de https://www.uregina.ca/student/registrar/assets/docs/pdf/exam-invigilator-guides/UofR-Exam_Security_Protocol.pdf

Top 5 Techniques to Make Secure Online Examination System (2020). Eklavvya. Second Point will help the most. Recuperado el 19 de Junio de 2020, de https://www.blog.epravesh.com/top-5-techniques-to-make-online-examination-system-secure/

Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (2016). NIST National Institute of Standards and Technology. Recuperado el 12 de Junio de 2020, de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

Trabajo desde casa: Medidas de ciberseguridad para hacer home office (2020). Centro de Ciberseguridad de la Ciudad Autónoma de Buenos Aires. https://www.ba-csirt.gob.ar/files/material-didactico/Home_office.pdf