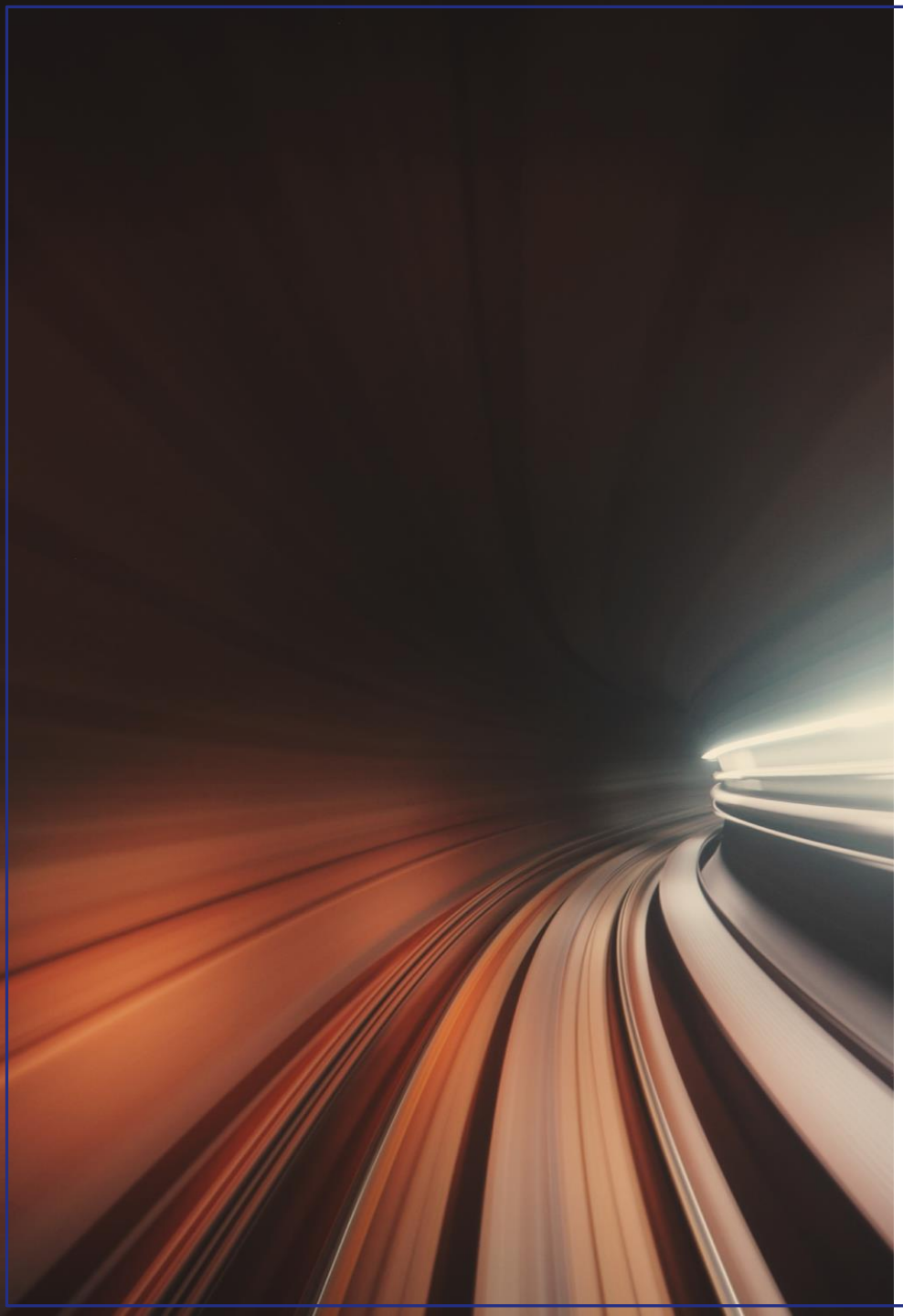

EcuaRE

CIBERSEGURIDAD EN TELETRABAJO

REASEGURADORA DEL ECUADOR

MAYO 2020



CONTENIDO

- EL TELETRAJO
- SEGURIDAD FISICA
- SEGURIDAD DIGITAL
- CONCIENTIZACION
- CONSEJOS DE SEGURIDAD EN CASA

TELETRABAJO

El teletrabajo, o trabajo a distancia, permite trabajar en un lugar diferente a la oficina. El trabajo se realiza en un lugar alejado de las oficinas centrales o de las instalaciones de producción, mediante la utilización de las nuevas tecnologías de la información y la comunicación.

El teletrabajo ha pasado de ser una alternativa a una obligación para la mayoría de ecuatorianos, por lo menos durante la duración del estado de emergencia. Contar con un espacio separado del resto de la casa y seguir una rutina como lo harías en la oficina son dos pilares para hacerlo con éxito. Pero, además, si queremos evitar problemas, también debemos considerar **revisar la seguridad informática** en casa para proteger bien nuestro trabajo.

SEGURIDAD FISICA

SEGURIDAD FISICA

A nivel corporativo

Pueden existir medidas y controles como cámaras, sensores, biométricos, reconocimientos de voz y una serie de medidas de seguridad digitales como firewalls, políticas de dominio, controles de acceso, cifrado de contraseñas que permiten blindar la red y por ende los activos de información

Pero y a nivel de la casa ?

Primero debemos garantizar un ambiente de trabajo propio y separado, no trabajar en locaciones inapropiadas como la cama. El ambiente de trabajo que hayamos elegido debe estar limpio y sanitizado en las superficies y debemos limpiarnos las manos antes y después de usarlos.

Se recomienda que en el espacio seleccionado no debamos involucrar a los niños y mascotas por seguridad del equipo y por ende de la información.

SEGURIDAD DIGITAL

Tecnología del hogar

Generalidades

Tener en consideración las características del ROUTER que tenemos instalado en casa y sobre todo tener mapeado que enlaces de comunicación tengo disponibles para acceder a los recursos de internet y a las tecnologías de la empresa: wifi, celular, etc.

Evitar escenarios que podrían generar una saturación a la red inalámbrica del hogar, lo que podría provocar menor calidad de señal en el internet al tener muchos dispositivos conectados y consumiendo el ancho de banda. Cuando se tenga videoconferencias se debe procurar contar con el mayor ancho de banda disponible.

Seguridad

Debemos configurar la red wifi con una contraseña segura, así como también la del administrador del ROUTER (en esta actividad podríamos solicitar asistencia de nuestro proveedor) con la finalidad de blindar nuestra red ante posibles ataques externos.

Acceso a recursos de la empresa

La empresa provee una VPN segura para acceso a los recursos y servicios de información en oficina, la contraseña de acceso a la VPN no deberán escribirla en físico o un archivo digital, porque puede quedar expuesta y por ende provocar robo de información.

Los ejecutivos que estén trabajando con equipos de la compañía no deberán instalar otros programas que los que estaban autorizados en la oficina.

Para los ejecutivos de la empresa que trabajan con equipos propios se recomienda tener software original de sistema operativo y de los diferentes aplicativos que utilicen o freeware con licencia de uso universal de fuentes confiables.

Evitar el uso de almacenamiento de dispositivos externos o pasarles antes de usarlo un software antivirus.

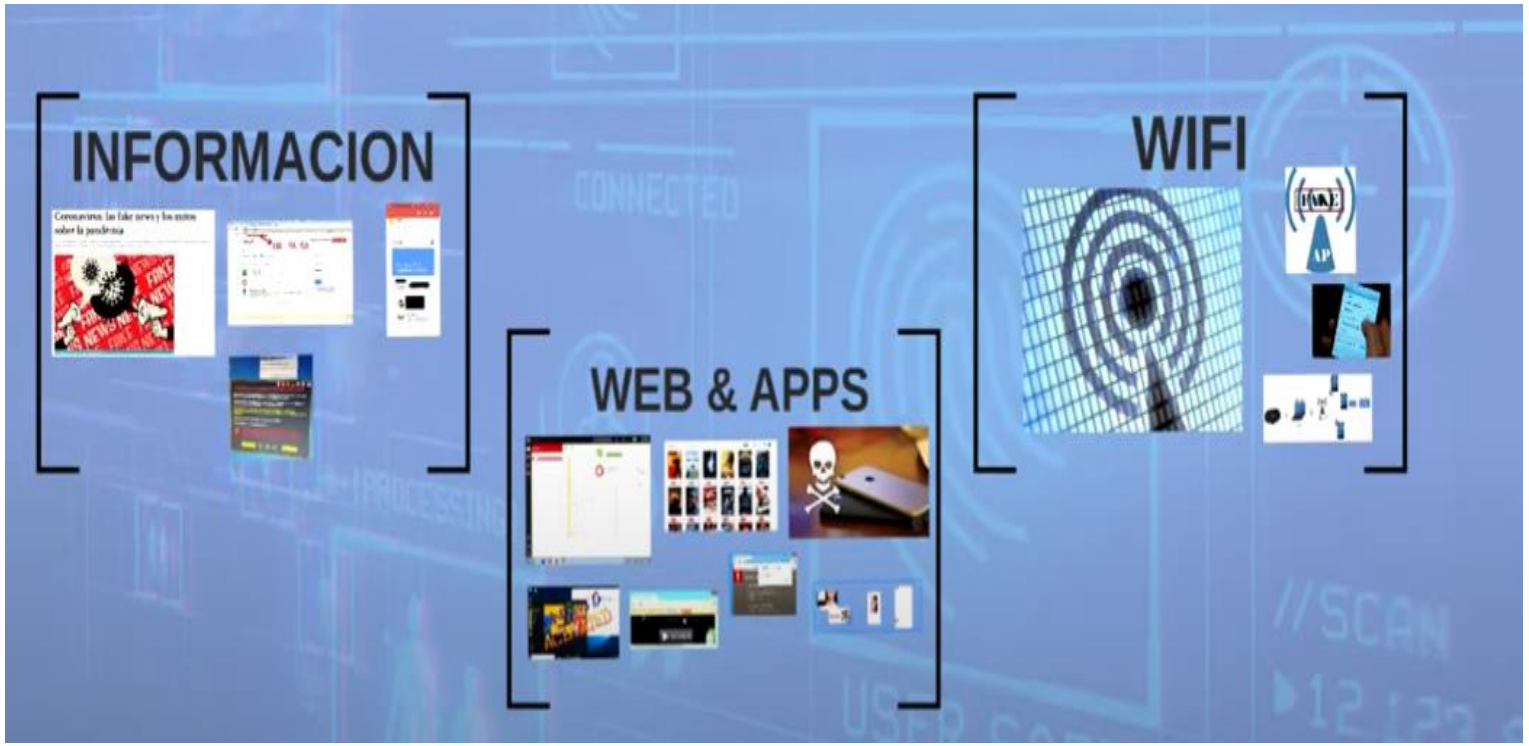
Herramientas colaborativas

Son herramientas que permiten compartir archivos para modificar entre varios usuarios como es el caso que nos ofrece el servicio de office 365.

El uso de estas herramientas deberán hacerlo con mucho cuidado para no viralizar, sobre todo al compartir archivos o subir archivos al almacenamiento en la nube que pueden contener virus.

Cuando recibamos documentos por medio de estas herramientas, debemos revisar que estén relacionados con temas que a su vez estén ligados directamente a un proceso de la empresa o que sea de interés general a la misma.

CONCIENTIZACION



Concientización

Considerar siempre que el origen de toda información que recibamos sea de fuentes confiables, y verificar si son reales. No leer FAKE NEWS ni acceder a sitios no autorizados.

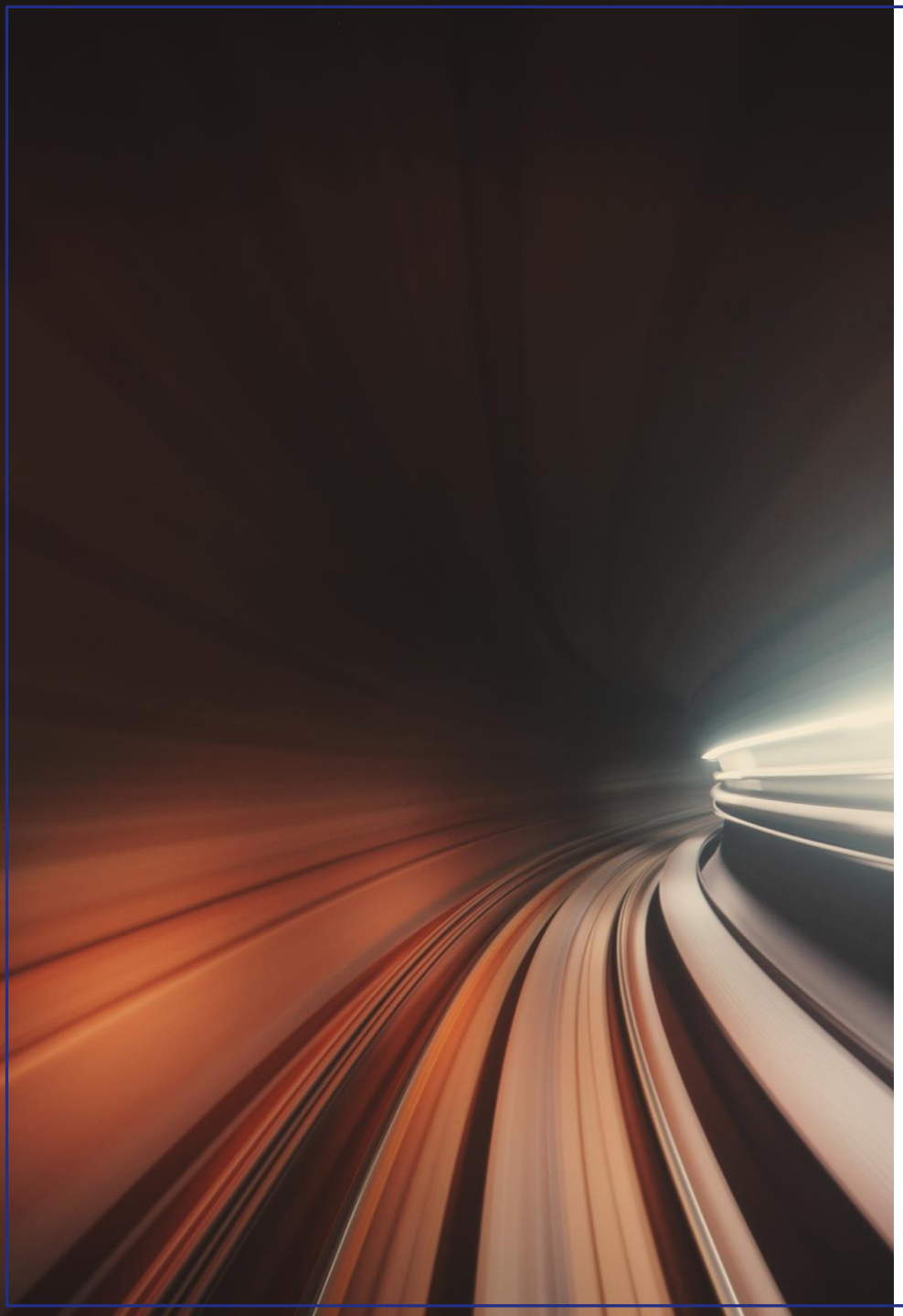
Si algún servicio o WEBSITE te solicita algún permiso para instalar alguna herramienta en tu equipo, deberás considerar si la fuente es confiable, caso contrario no instalarlo.

Muchos ataques de PHISING (suplantación de identidad) se están dando por emails que recibimos, no debemos abrirlos cuando su origen o asunto sea sospechoso, y jamás cambiar una clave de acceso desde un link que nos ha llegado a nuestro correo.

No instalar software pirata no licenciado y en caso de necesitarlo, procurar instalarlo en una máquina virtual.

No instalar nada que le solicite paginas de STREAMING que no son de pago.

No conectarnos a ACCESS POINT de redes que no nos pertenecen porque pueden ser redes no seguras (públicas).



CONSEJOS DE SEGURIDAD EN CASA

1. Proteger tus contraseñas: verificación en dos pasos
2. Seguridad para tu ordenador: antivirus y firewall
3. Mantener tu sistema y programas siempre actualizados
4. Proteger tu ROUTER y conseguir una Wi-Fi más segura
5. Utiliza una conexión VPN para teletrabajar
6. Ignora el spam y los emails con objetivo “PHISING”
7. Precauciones de seguridad informática también en el móvil

Seguridad Activa y Pasiva

La **seguridad activa es la primera línea de defensa**. Engloba todas las acciones que puedes llevar a cabo para evitar “contagiarte”, desde tener el antivirus actualizado hasta contar con contraseñas fuertes, no abrir enlaces desconocidos o de sitios sospechosos, o analizar los USB que vayas a utilizar.

La seguridad pasiva entra en funcionamiento una vez que tu equipo ha sido infectado. En este punto, el objetivo es minimizar los efectos del virus con medidas como escanear el equipo para intentar eliminar el virus o usar las copias de seguridad que tengamos para poder formatear el ordenador y restaurar los archivos.

1. Proteger tus contraseñas: verificación en dos pasos

Las contraseñas protegen tu información más sensible, a la que más le interesa acceder a los hackers informáticos. **Lo más básico es contar con una contraseña fuerte,** que incluya mayúsculas, minúsculas, símbolos y números; pero también que evite patrones de teclado, como *1234*, *qwerty* o nombres comunes y fechas.

Sin embargo, la acción más útil es **implementar un sistema de verificación en dos pasos**. Básicamente consiste un paso adicional, un código más que debes poner después de tu usuario y contraseña. Esta doble autentificación se puede realizar por SMS, lo más habitual, o con aplicaciones específicas para ello como Google Autenticador, por mencionar una de las más populares.

2. Seguridad para tu ordenador: antivirus y Firewall

El antivirus es la protección básica que todo sistema debería tener. Su misión es detectar amenazas para tu equipo y bloquearlas. La oferta en el mercado es enorme e incluso **hay opciones gratuitas muy fiables** como las que ofrecen **Avira**, **Avast** o **AVG**, no se recomienda la protección del Windows Defender que incluye el sistema de Microsoft. Sin embargo las licencias de pago siempre serán más confiables porque ofrecen un sinnúmero de opciones y servicios adicionales para proteger de mejor manera a tu equipo.

Por su parte, el firewall o cortafuegos controla el acceso a la red del ordenador. Su misión es proteger la información que guarda el equipo bloqueando los ataques de quienes quieren acceder a ella, entre otras cosas.

Windows incluye su propio cortafuegos, pero si quieres, puedes instalar uno alternativo. Entre las opciones gratuitas destacan **Zone Alarm** o **Comodo**, aunque los antivirus antes mencionados también permiten activar su propio firewall.

3. Mantener tu sistema y programas siempre actualizados

Si hay algo en lo que Windows insistirá hasta la saciedad es que **actualices tu sistema**. Te lo recordará una y otra vez hasta que lo hagas, y no es por casualidad. Mantener tu sistema y programas actualizados es una de las mejores maneras de evitar vulnerabilidades.

Y es que **buena parte de las actualizaciones están centradas en mejorar la seguridad del sistema**. Son la respuesta de los fabricantes a las nuevas fórmulas que los ciberdelincuentes van encontrando para atacar tu equipo.

4. Proteger tu Router y conseguir una Wi-Fi más segura

El Router es el punto de acceso de internet en tu casa. Entre otras cosas, es el encargado de distribuir la señal Wifi por la casa. Por eso mismo debes protegerlo para proteger los equipos de casa y evitar también que te “roben” el Wifi.

Estas son **cuatro formas de conseguirlo**:

Cambia el nombre de tu Wifi. Nunca deberías mantener los valores de fábrica del router. Empieza por modificar el SSID de la Wifi (el nombre que se ve al buscarla) para que los posibles hackers no puedan identificar tan fácil tu operador y el modelo de router concreto.

Cambia la contraseña. Busca una contraseña diferente que contenga números, mayúsculas, minúsculas y símbolos.

Mejora el cifrado de la red Wifi. Apuesta por el máximo nivel de seguridad con un cifrado WPA2 frente a las modalidades WEP, mucho menos seguras. Esto puedes hacerlo entrando en la configuración de la red del Router desde tu dispositivo. Las instrucciones de cómo hacerlo suelen venir en el manual.

4. Proteger tu Router y conseguir una Wi-Fi más segura

Activa el filtrado MAC. El filtrado MAC es simplemente una lista blanca o negra de dispositivos que pueden y no pueden acceder a tu Wifi. Es una buena manera de controlar quién usa la red. Si no quieres llegar hasta este extremo, sí que deberías por lo menos comprobar qué equipos se conectan a tu red. Una forma de hacerlo es darle a cada uno de los equipos un nombre sencillo con el que puedas indentificarlo fácilmentemente desde el menú de configuración de tu Router.

5. Utiliza una conexión VPN para teletrabajar

Una VPN es una **tecnología que se usa para conectar uno o más equipos a una red privada a través de internet.** Son las redes que las empresas utilizan para dar acceso a sus archivos a los empleados que teletrabajan.

Puedes acceder a este servicio a través de herramientas que te haya provisto la empresa, las cuales han de proporcionarte un usuario y contraseña para que puedas acceder a los recursos de una manera segura y cifrada.

6. Ignora el spam y los emails con objetivo “Phising”

Aunque cueste admitirlo, **somos uno de los eslabones más débiles de la cadena de seguridad** de los equipos informáticos. Los hackers lo saben y también buscan nuevas fórmulas de explotar esa debilidad, especialmente a través del correo electrónico.

El primer paso para evitar el spam es no llegar ni siquiera a recibirlo. La mayoría de correos electrónicos cuenta con sus propios sistemas para detectar spam. Puedes ayudarle marcando como spam los correos que ya hayas detectado que lo son.

Además, para **saber si un correo es spam** puedes usar estos cinco indicadores:

1. El remitente no corresponde con el servicio que envía el correo. Por ejemplo, cuando una empresa usa un correo de GMAIL u otro similar en vez de con el dominio de la empresa.
2. Mensajes con fallos gramaticales u ortográficos.
3. Correos de servicios que no has utilizado o contratado.
4. Archivos adjuntos que en realidad son ejecutables. Estos archivos se camuflan normalmente en archivos comprimidos.

6. Ignora el spam y los emails con objetivo “Phising”

5. Mensajes de entidades financieras pidiendo que confirmes tu clave. Esta es una de las estafas más repetidas. La mayoría de entidades no te pedirá nunca que lo hagas por correo.

La mejor fórmula para evitar el PHISING, es **no abrir los enlaces sospechosos** y, ante la duda, acudir a la página oficial del servicio o entidad que nos envía el email tecleando la URL en el navegador. En este punto, **el mejor antivirus para tu ordenador eres tú.**

7. Precauciones de seguridad informática también en el móvil

El ordenador no es el único dispositivo que necesita seguridad al teletrabajar. El móvil también es vulnerable a los ataques. Empieza por contar con un antivirus, si es que el fabricante no incluye ya uno.

Al igual que en el caso anterior, **mantén actualizadas las aplicaciones y el sistema operativo** para evitar vulnerabilidades y apuesta por contraseñas seguras. Al final, tu móvil no deja de ser un pequeño ordenador que también necesita su propia seguridad.

Sigue estas indicaciones y podrás teletrabajar en casa de forma segura para tus equipos y tu información.


EcuaRE