

CIBERGUÍA - NAVEGAR POR EL CIBER-ESPACIO CON PREVENCIÓN Y SEGURIDAD



CIBERGUÍA- NAVEGAR POR EL CIBERESPACIO CON PREVENCIÓN Y SEGURIDAD



Fuente: Secretaría de Seguridad y Protección Ciudadana

Hoy en día, el uso de las tecnologías de la información y comunicación son de suma importancia para el desarrollo de las actividades diarias de la sociedad en general. A través de ellas se han facilitado muchos aspectos de la vida cotidiana. Sin embargo, esta facilidad que nos proporciona el ciberespacio, también trae consigo riesgos que, en muchas ocasiones, sin darnos cuenta pueden ocasionar daños, tanto en el trabajo como en la vida personal e incluso en la economía. En ese sentido, la Secretaría de Seguridad y Protección Ciudadana, refrenda el compromiso que tiene con la sociedad, y por ello presenta a través de la Cibergrafía, diferentes herramientas para facilitar la comprensión de conceptos relacionados a la ciberseguridad. De esta manera, ofrece orientación para evitar ser víctimas de los delincuentes y datos de contacto ciudadano para reportar incidentes cibernéticos.

Liga de consulta:<https://www.ipn.mx/assets/files/cenac/docs/ciberseguridad/Ciberguia-2021.pdf>

CIBERGUÍA- NAVEGAR INTERNET CON PREVENCIÓN Y SEGURIDAD

Teletrabajo y sus beneficios

TELETRABAJO: Es un recurso que se apoya de la tecnología digital para que las y los empleados realicen sus labores sin presentarse físicamente en sus centros de trabajo.

El factor determinante que ha impulsado la transformación digital de todos los sectores es el distanciamiento social, a causa del Coronavirus.

Beneficios del TELETRABAJO:



FLEXIBILIDAD DE HORARIO
para compaginar la vida
laboral y familiar.



INSERCIÓN LABORAL
para las personas con
dificultades de movilidad.



MENOR ESTRÉS



AHORRO DE TIEMPO Y DINERO
en traslados a los centros de
trabajo. Reducción del uso
de recursos en las instalaciones.



REDUCCIÓN DEL TRÁNSITO
y descongestión en los
servicios de transporte
público.

Sin embargo, el
teletrabajo
también tiene
áreas de
OPORTUNIDAD
que dependen
en gran parte
de quien
lo ejerce.

CIBERGUÍA- NAVEGAR INTERNET CON PREVENCIÓN Y SEGURIDAD



Problemas asociados al teletrabajo

Trabajar remotamente sin seguir las pautas de seguridad genera un riesgo para las y los empleados o servidores públicos, lo cual puede ser aprovechado por los cibercriminales de la siguiente forma:

1 INFECTAN NUESTROS DISPOSITIVOS CON PROGRAMAS DAÑINOS

2 ROBAN, ALTERAN LA INFORMACIÓN QUE USAMOS

3 SUSTRAYEN NUESTRA IDENTIDAD Y PUEDEN DIFAMARNOS

4 DEFRAUDAN

5 ESPÍAN

Medidas para evitar riesgos en el teletrabajo

1 USAR ANTIVIRUS

2 MANTENER ACTUALIZADOS TODOS LOS PROGRAMAS considerando aplicaciones, navegadores web y sistemas operativos.

3 RESPALDAR LOS ARCHIVOS en medios de almacenamiento externos o en la nube.

4 USAR CONTRASEÑAS SEGURAS diferentes y para todos los dispositivos.

5 ENCRIPRAR equipos y medios de almacenamiento utilizados.

6 USAR LLAVEROS ELECTRÓNICOS para guardar usuarios y contraseñas.

7 RESGUARDAR USUARIOS Y CONTRASEÑAS en los lugares de trabajo.

8 CUIDAR DISPOSITIVOS O MEDIOS DE ALMACENAMIENTO en lugares públicos.

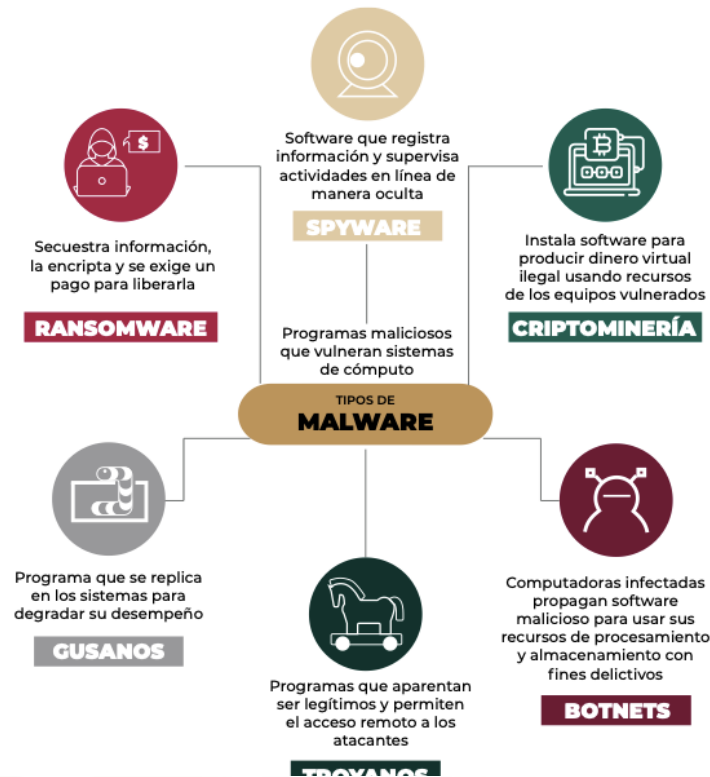


CIBERGUÍA- NAVEGAR INTERNET CON PREVENCIÓN Y SEGURIDAD

POR UNA NAVEGACIÓN SEGURA, QUE LA SEGURIDAD Y PROTECCIÓN EN EL CIBERESPACIO SE VUELVA CULTURA

¿Qué es un programa dañino (Malware)?

Existen distintos tipos de programas informáticos, pero hay uno que está diseñado para generar daño en ese entorno de funcionamiento habitual, y a ese se le denomina software malintencionado o MALWARE:



CIBERGUÍA- NAVEGAR INTERNET CON PREVENCIÓN Y SEGURIDAD

POR UNA NAVEGACIÓN SEGURA, QUE LA SEGURIDAD Y PROTECCIÓN EN EL CIBERESPACIO SE VUELVA CULTURA

Afortunadamente
PODEMOS PREVENIRLO

Recomendaciones para evitar ser víctima del Ransomware



Desactiva la reproducción automática de dispositivos de almacenamiento externo, como discos y USB.



No confíes en correos con programas o archivos ejecutables adjuntos, presta atención a su extensión.



Evita el software ilegal y pirata, ya que puede contener Malware.



Usa cuentas de usuarios sin permisos de administrador.



Mantén los programas y el sistema operativo actualizados.



Haz copias de seguridad de tu información periódicamente.



Si recibes archivos, anuncios o enlaces no esperados, pregunta a la persona si los ha enviado. El sistema podría infectar y propagar el Malware.



Instala un antivirus con capacidad proactiva de detección.

GRACIAS



EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

AEF CIUDAD **MÉXICO**
AUTORIDAD EDUCATIVA FEDERAL EN LA CIUDAD DE MÉXICO



2022 *Ricardo Flores*
Año de Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA