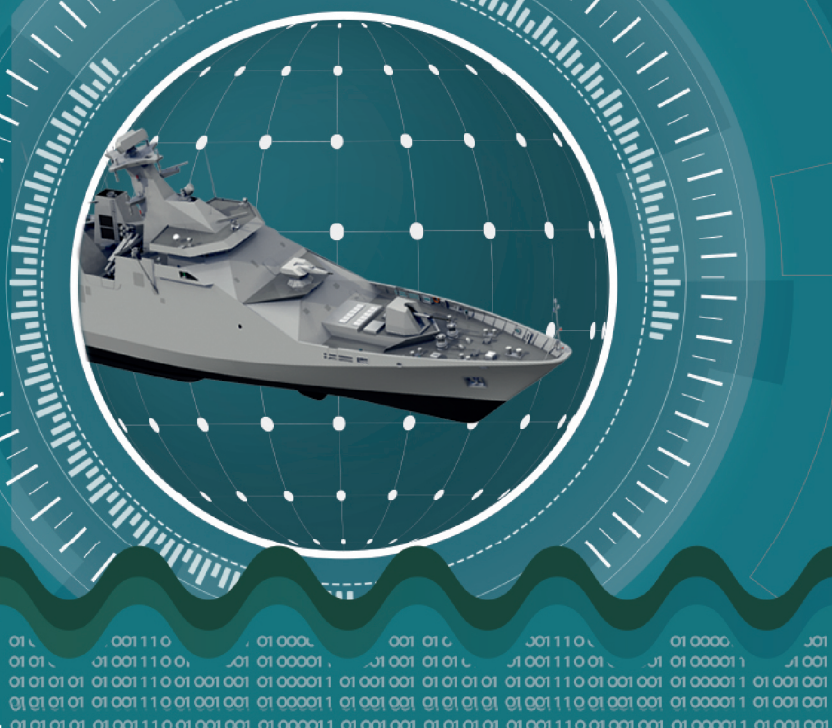
GOBIERNO DE MÉXICO

MARINA
SECRETARÍA DE MARINA

CARTILLA DE CIBERSEGURIDAD DE LA SECRETARÍA DE MARINA



“SEGURIDAD Y DEFENSA EN EL CIBERESPACIO”

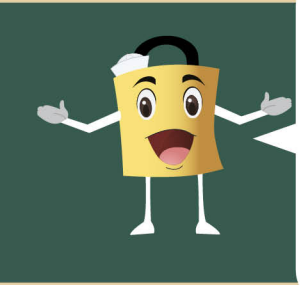
Mensaje del
Almirante Secretario de Marina

Personal naval y civil de la institución: el ciberespacio es considerado por las Fuerzas Armadas como el quinto campo de batalla, paralelo y transversal al entorno marítimo, aéreo, terrestre y espacial. El ciberespacio representa un gran beneficio para la humanidad y en él convergen gobiernos, iniciativa privada y sociedad, pero también es usado por actores malintencionados que generan amenazas y riesgos, dando paso a los ataques cibernéticos que cada vez son más frecuentes y sofisticados.

La institución, al ser una instancia de Seguridad Nacional del Estado Mexicano, tiene la responsabilidad de proporcionar seguridad a este entorno operacional, desde el ámbito de sus atribuciones.

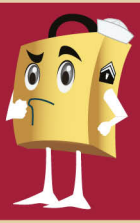
Para alcanzar la seguridad en el ciberespacio se necesita que todos y cada uno de nosotros conozcamos los riesgos y amenazas existentes, por lo que les instruyo para que apliquemos las medidas básicas de ciberseguridad a efecto de proteger nuestros activos de información.

Almirante José Rafael Ojeda Durán



¡¡¡Hola!!! soy “Cibercito” y te acompañaré a conocer la cartilla de ciberseguridad de la MARINA, la cual tiene como objetivo concientizar a todo el personal naval y civil, sobre la existencia de amenazas y riesgos, a las que nos encontramos expuestos cuando estamos conectados al ciberespacio.

¡¡¡Mucho ojo!!! Si alguno de los conceptos que aquí menciono no te son familiares, te invito a consultar el glosario que se encuentra al final de la cartilla, para que no estés desactualizado.



Si tú eres naval o civil que emplea las Tecnologías de Información y Comunicación (TIC) institucionales, como herramienta de trabajo diario, es de especial relevancia que comprendas y apliques los conceptos y recomendaciones que aqui se citan.

¿Sabes qué unidad de la Armada de México está generando capacidades de seguridad en el ciberespacio para beneficio de la sociedad?

Por si no lo sabes o eres de nuevo ingreso, te lo menciono. Se llama "Unidad de Ciberseguridad (UNICIBER)" y las capacidades que está desarrollando son: Seguridad de la Información, Ciberseguridad y Ciberdefensa.

Los tres conceptos tienen sus diferencias; ¡¡¡no te confundas!!!

La ***Seguridad de la Información*** es el conjunto de políticas de uso de las TIC, difusión de cultura y buenas prácticas para el resguardo y protección de la información.

La ***Ciberseguridad*** se aplica para la protección de la infraestructura tecnológica crítica del país (sector salud, energético, alimentación, agua potable, financiero, etc.), incluida la de MARINA. En este punto es donde se sitúa la gran familia naval, por lo que es recomendable que también conozcas los conceptos y medidas de seguridad que debes adoptar para que no seas víctima de las amenazas cibernéticas.

La ***Ciberdefensa*** es una atribución exclusiva de las Fuerzas Armadas, en materia de Seguridad Nacional, a través del ciberespacio.

De los términos anteriores nos centraremos en el de ***Ciberseguridad***.

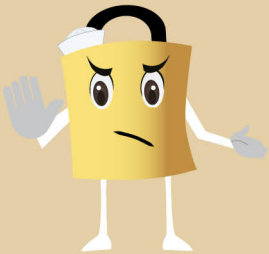
Seguramente te estarás preguntando ¿Cómo te puedes conectar al ciberespacio?

La respuesta es muy sencilla, es por medio de las TIC, es decir, a través de computadoras, teléfonos inteligentes, tabletas electrónicas, televisores inteligentes, cámaras fotográficas y todo medio tecnológico que nos brinde acceso o conectividad a internet.

Todos los equipos tecnológicos anteriores y muchos otros más, son empleados para facilitar las labores diarias del personal en cumplimiento de la misión institucional por los grandes beneficios que nos brindan.

Pero, ¿ya conoces las amenazas a las que te expones?

A continuación, te menciono las amenazas más comunes a las que te expones, no solamente tú como servidor público, sino también **¡tu familia!**, por lo que es importante que las tengas siempre presente cada vez que te conectas a internet.



CUIDADO

¿Sabes cómo ocurre un ciberataque? El atacante realiza lo siguiente:

1. Reconocimiento

Recolecta información de la víctima en fuentes abiertas (perfil de "**redes sociales**", páginas web, etc.)

Con la información que tiene elige la técnica de ataque para engañar al usuario.

2. Análisis

3. Implantación

Inyecta el código o agente malicioso a través de correos electrónicos y/o mensajes

Aprovecha la curiosidad, morbo o desconocimiento del usuario, para que descargue y ejecute un archivo (carpeta comprimida, link, etc.)

4. Explotación

5. Replicación

El código malicioso descargado buscará replicarse en el sistema o red para dañar la información.

El atacante logró robar la información, credenciales o dañar el funcionamiento de un sistema.

6. Impacto

¡¡¡Acuérdate que es nuestro compromiso cuidar la infraestructura tecnológica de la Institución!!!

Cuidados del correo electrónico

Si tú eres un usuario del correo naval con terminación "@semar.gob.mx" ¡¡¡Ten mucho cuidado!!!, este es el medio principal por donde pueden robar la información institucional.

Como usuario responsable del correo electrónico, antes de abrir un mensaje pregúntate: ¿Estoy esperando una información de algún remitente?

Si no es el caso, no abras correos de remitentes desconocidos ni tampoco hagas clic en enlaces con acortadores (https://bit.ly/2XftLTk o https://cutt.ly/gW0l1C2); estos enlaces redireccionan a páginas web, que en la mayoría de los casos contienen código malicioso que roban usuarios y contraseñas.

No descargues archivos comprimidos, con terminación zip o rar (TuFactura.zip o TuCotización.rar) de remitentes desconocidos y siempre asegúrate de que el antivirus de tu equipo esté actualizado, ya que las actualizaciones son los parches de seguridad.

PHISHING

¿Qué es?

Estafa cometida a través de correos basura (spam) o suplantación de páginas web, mediante el cual, el estafador intenta conseguir de forma fraudulenta, cuentas de usuarios legítimos, contraseña y datos bancarios, entre otra información confidencial.

Consecuencias del Phishing:

- Robo de datos personales.
- Robo de Información financiera.
- Robo de credenciales de acceso.
- Suplantación de identidad.

¿Cómo evitar el PHISHING?

- No abrir correos electrónicos de remitentes desconocidos.
- Evitar abrir o visualizar archivos adjuntos de remitentes desconocidos.
- No pulsar en links de sitios web de bancos, incluidos en correos electrónicos y/o mensajes.
- Mantener actualizado el Antivirus.

VISHING

Voice Phishing Scam

¡ALERTA!

¿Sabes qué es el **vishing?**

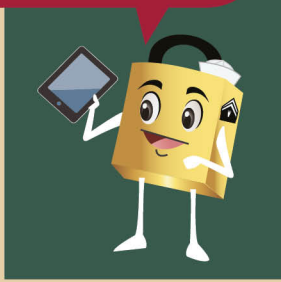
Es el delito de **engañar** a las personas para que compartan información confidencial, como contraseñas y números de tarjetas de crédito; otro de los objetivos es la estafa de dinero.

También se da por **suplantación de identidad por voz o SMS**

¿Cómo evitar ser víctima del vishing?

- **Desconfía.**
- **Mantente alerta.**
- **Verifica la identidad de la persona que te contacta. y NO realices ninguna acción que te pida.**
- **Pídele más información, NO LA DES TU.**
- **Informa a tu superior y toma medidas.**
- **¡¡¡CUIDA TU INFORMACIÓN!!!**

Ahora que ya conoces algunos de los riesgos, te doy unas recomendaciones muy sencillas, que te ayudarán a navegar seguro en tu área laboral y con tu familia.



Seguridad en tus redes sociales

- Utiliza contraseñas robustas.
- No compartas fotografías de tus actividades laborales.
- No publiques o difundas videos que ridiculicen a la institución.
- Evita enviar fotografías de estados de cuenta y otra información financiera.
- Evita crear o fomentar rumores del personal de la institución.
- Configura la privacidad de tus dispositivos (computadora, teléfono, tableta, etc.) para que no compartan de manera predeterminada su ubicación.
- No te conectes a redes WIFI públicas para abrir tus redes sociales.

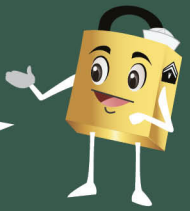
¡Recuerda que todos somos una gran familia naval!

Buenas prácticas en los equipos de cómputo institucionales, para evitar Incidentes de Ciberseguridad

- Mantén siempre tu antivirus actualizado.
- No instales software no autorizado.
- No conectes dispositivos de almacenamiento no autorizados (USB) en los equipos de cómputo.
- No emplees las nubes de almacenamiento para respaldar información institucional, sin las medidas de protección de cifrado.
- No conectes equipos de cómputo personales, sin autorización a la Red Informática Institucional.
- Recuerda no utilizar los equipos institucionales para revisar tus redes sociales.
- No veas contenido multimedia gratuito en sitios desconocidos.
- Emplea sólo aplicaciones autorizadas y con licencia.

¡Con tu participación logramos mucho!

Nunca debes olvidar el Decálogo de Seguridad de la Información



1. Pensar, actuar, comportarse y expresarse en armonía con la legislación, normatividad y los valores institucionales.

2. Entender que la Seguridad de la Información es un asunto de todos, personal naval y civil.

3. Preservar la reserva y confidencialidad de la información.

4. No utilizar la información a que se tenga acceso, para beneficio personal o de terceros.

5. No proporcionar información que vulnere la confidencialidad o dañe la imagen institucional.

6. Apoyar a tu Mando, previniendo, detectando y respondiendo a eventos e incidentes de Seguridad de la Información en los actos dentro y fuera del servicio.

7. Emplear las TIC e internet institucionales, únicamente para fines del servicio.

8. No alterar información para encubrir anomalías, generar rumores en redes sociales o participar en la planeación o ejecución de actos deshonestos.

9. Evitar que personas no autorizadas ingresen a las áreas de protección y resguardo de información.

10. No emplear programas sin licencia de uso, respetando siempre los derechos de autor y evitando la piratería.

Glosario

Antivirus: software elaborado para la protección de un sistema.

Cifrado: transformación de datos para ocultarlos.

Firewall: hardware o software diseñado para la seguridad de la red, controlando los accesos a ella.

Hacker: persona que accede sin autorización a un sistema informático de una manera malintencionada.

Malware: software diseñado para comprometer un sistema y permitir la explotación de vulnerabilidades.

Parche de seguridad: actualizaciones periódicas de software para corregir fallas y vulnerabilidades.

Robo de información: acceso no autorizado a datos.

Spyware: software diseñado para espiar un sistema y enviar los datos sin autorización.

Virus: malware diseñado para propagarse automáticamente en un sistema o una red.

Vulnerabilidad: es una debilidad que tiene un sistema y que puede poner en peligro toda una red informática.

Puntos de contacto para el personal naval y civil que labora en la SEMAR:

Unidad de Ciberseguridad
EMGA-UNICIBER
CSIRT-SEMAR

uniciber@semar.gob.mx
uniciber.ciberincidentes@semar.gob.mx

Accede a nuestro portal en internet:
https://www.gob.mx/semar/articulos/unidad-de-ciberseguridad-279197?idiom=es