

 DIPLOMADO EN
CIBERSEGURIDAD

CONTROLES EN CIBERSEGURIDAD ESSENTIALS

Los activos de información y la triada CID

La famosa triada...

De acuerdo a lo visto hasta ahora, gran parte de los activos de información pueden verse amenazados interna o externamente, pero ¿cómo los activos de información podrían analizarse desde la triada CID?

Confidencialidad

- La información sólo puede ser accedida por personal previamente autorizado.

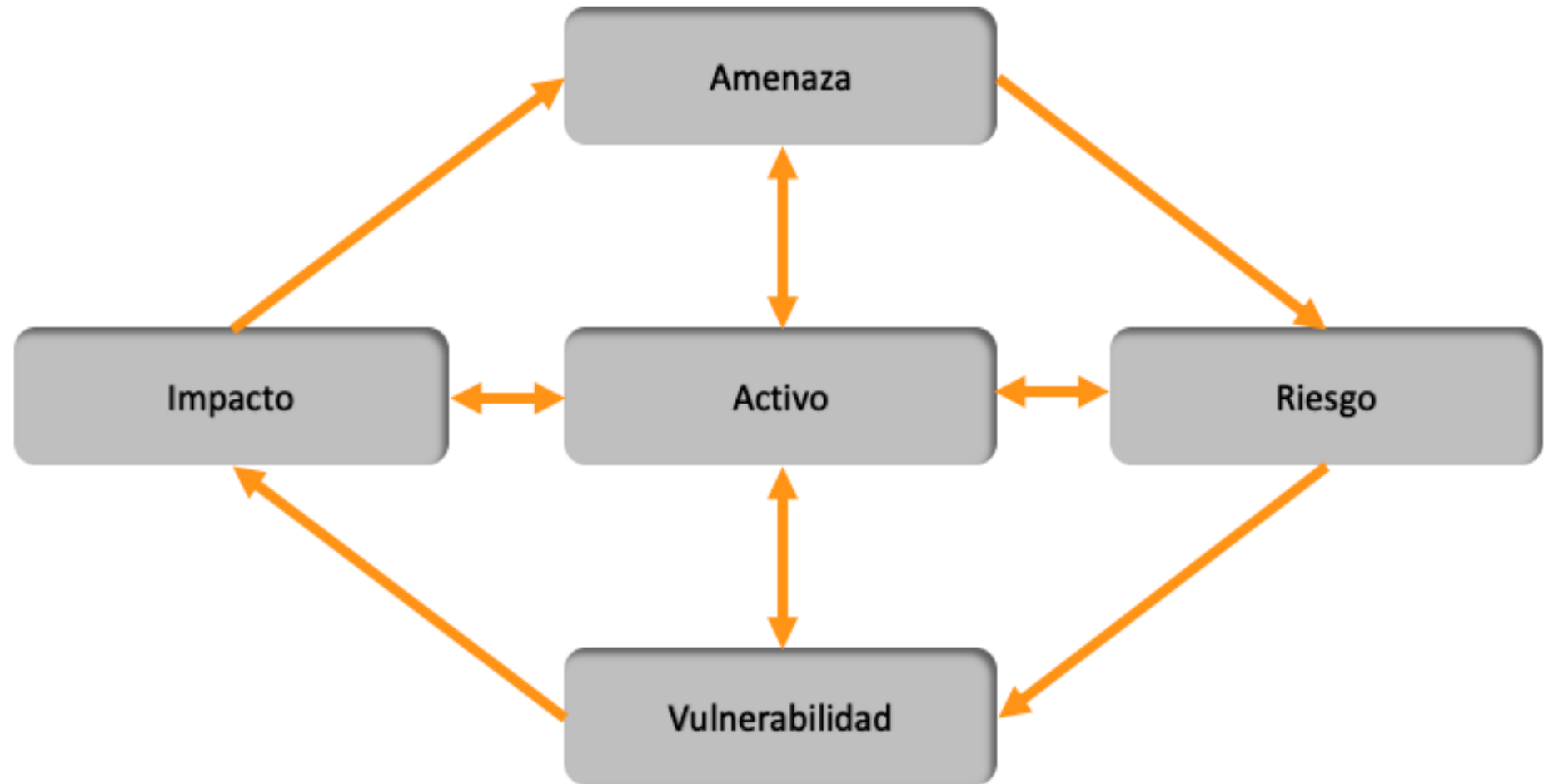
Integridad

- La información debe mantenerse intacta, incorrupta, sin modificaciones desde origen hasta su destino.

Disponibilidad

- La información debe estar disponible 24 x 7 x 365..

Volviendo a los activos de información



Riesgo

¿Qué es el riesgo?



Es la posibilidad que ocurra un acontecimiento que tenga un impacto negativo.

Dos dimensiones de riesgo



- **Probabilidad:** La posibilidad de que un evento se produzca.
- **Impacto:** Las consecuencias que se podrían generar como consecuencia de ese evento.
- **Riesgo = Impacto x Probabilidad**

Gestión de activos de información

Gestión de activos de información



Gestión de activos de información tangibles



Ejemplo

Un funcionario está a cargo de un laboratorio de computación de una institución educacional, este laboratorio está cerca de los baños del piso.

¿Qué riesgos corre el funcionario?

Que ocurra un derrame de agua en el piso que pueda afectar a la parte eléctrica del laboratorio

Que no tenga respaldo de la información

Que entre un malware en la red.



Ejemplo

El funcionario toma conciencia de estos riesgos, por lo que decide hablar, tanto con el prevencionista de riesgos de la institución, como con el encargado de informática y redes, expone la situación, por lo que el prevencionista decide evaluar los riesgos y entregar un informe detallado de éstos.

El encargado de informática y redes, toma conciencia y decide comenzar a evaluar soluciones de backup, HA, antivirus, y también, segmentación de red.



Ejemplo

El funcionario ahora cuenta con una política de respaldos, además de que la red del laboratorio se encuentra separada de la red Organizacional, evitando así, un ingreso de Malware que podría afectar a ésta, cuenta también, con un Playbook que le ayudará a saber como actuar ante distintas situaciones. Finalmente, la organización también cuenta con políticas de prevención de riesgos físicos y del entorno, señala los accesos y también, se sabe como actuar antes distintos incidentes relacionados

Gestión de activos de información intangibles



Ejemplo

Supongamos que un funcionario está a cargo de mantener el listado de usuarios, la que maneja en una Planilla de Excel ¿Qué riesgos corre el funcionario?

- Fuga de información
- Integridad de datos
- Pérdida de información confidencial
- Incluso, sufrir un ataque de Malware que comprometa esta información.

Entre otros...



Ejemplo

El funcionario es consciente de estos riesgos, por lo que decide hablar con su supervisor y le indica éstos, comentándole que lo que debería realizar la Organización es mantener esta información sensible no en una planilla, sino que en una BD como AD, por ejemplo, además, comenta que es importante manejar los accesos a través de una bóveda, y designar a un custodio que se comprometa a guardar y proteger la información.

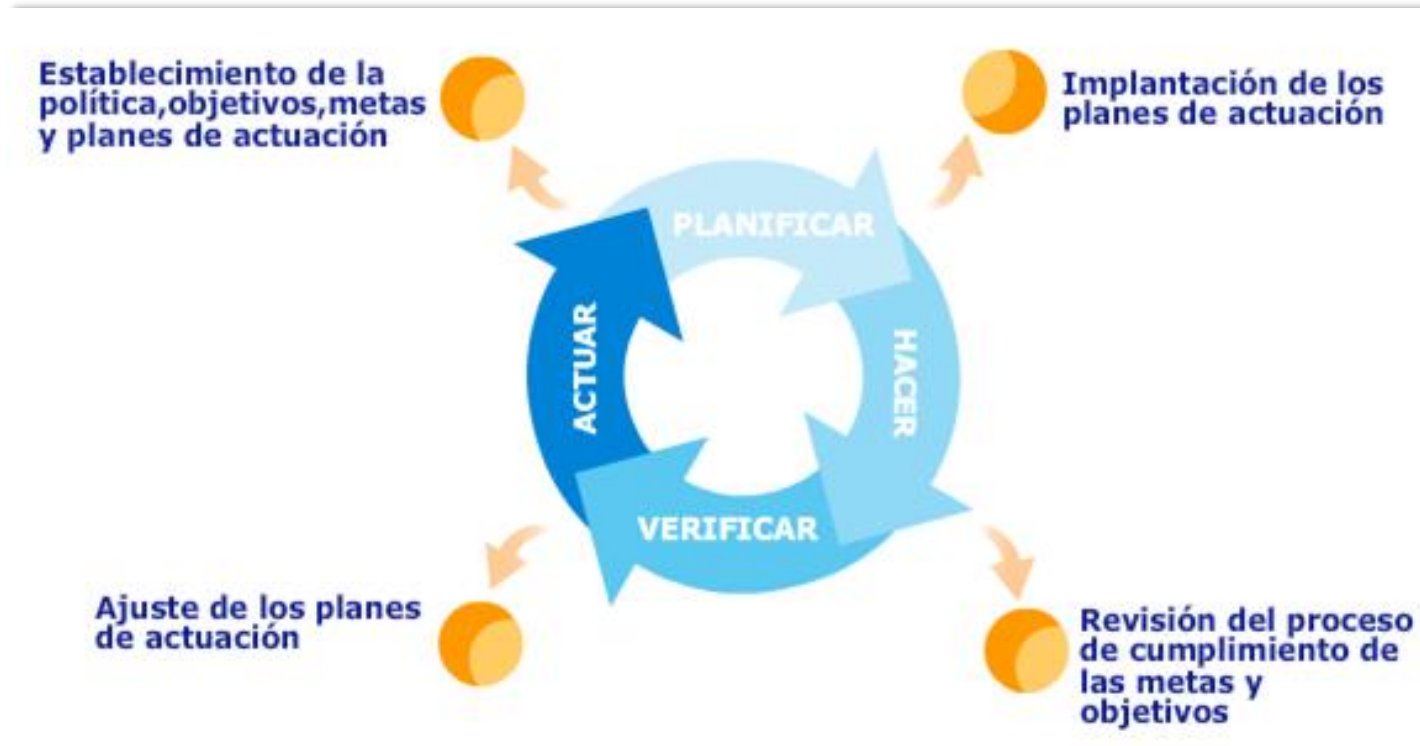


Ejemplo

El funcionario ahora cuenta con una bóveda que administra las cuentas, sobre todo las de altos privilegios, además, generó en conjunto con su equipo una política de control de cuentas, todas las cuentas de la Organización se trabajan en un AD, que se conecta a los servidores que sostienen la bóveda, se rige bajo políticas e incluso normativas, y logró minimizar los riesgos asociados.

El modelo PDCA

PDCA



Dado por entendido que estamos trabajando con un enfoque en procesos es que podemos aplicar la metodología conocida como PDCA (Plan-Do-Check-Act) o en español PHVA (Planificar-Hacer-Verificar-Actuar) que es un sistema de mejora continua.

Metodología PDCA: Plan - Planificar

Establecer los objetivos y procesos necesarios para obtener los resultados de acuerdo con el resultado esperado. Al tomar como foco el resultado esperado, difiere de otras técnicas en las que el logro o la precisión de la especificación es también parte de la mejora.



Metodología PDCA: Do - Hacer



Es la etapa de proceso en la que es necesario gestionar de forma adecuada todos los recursos de la empresa.

Metodología PDCA: Check - Verificar



Todos los procesos deben ser analizados y medidos, de forma que cumplan siempre con los requisitos, políticas y objetivos de la organización

Metodología PDCA: Act - Actuar



Una vez realizados los análisis de los resultados producidos, se deben adoptar las medidas adecuadas y planificar nuevamente con el fin de obtener una mejora continua.

Conceptos clave para la Seguridad de la Información

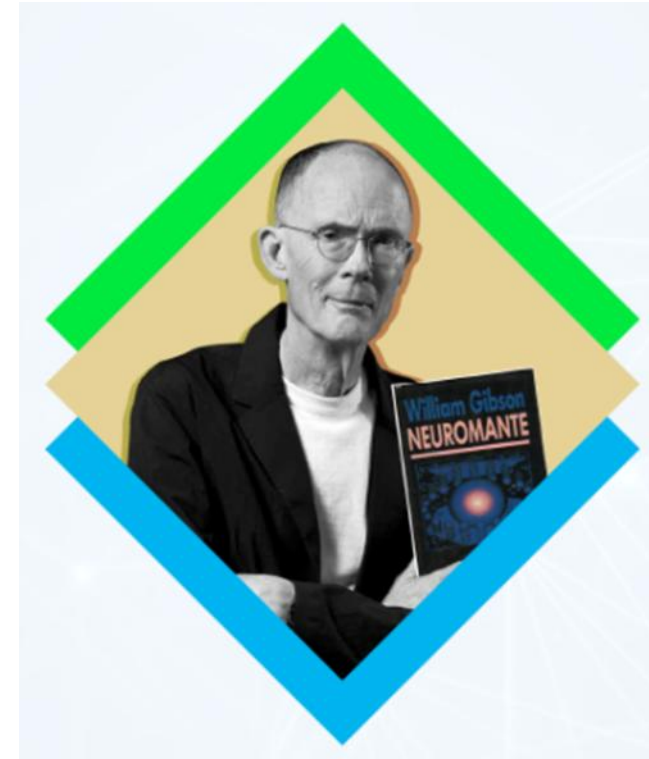
Conceptos clave para la gestión de la Seguridad de la Información




¿Qué es el Ciberespacio?

Ciberespacio

En el año 1984, William Gibson, en su novela "Neuromante" nos introducía en el concepto de "Ciberespacio", concepto que, claramente, presenta diversos matices de nuestra realidad actual, sin embargo, no es del todo alejado de nuestras vidas, sino que es ya algo propio, pues todos nosotros(as) ya tenemos una gran presencia en el Ciberespacio.



Algunas definiciones de Ciberespacio



Es el dominio global dentro del entorno de información que consiste en la red interdependiente de infraestructuras de sistemas de información que incluye Internet, redes de telecomunicaciones, sistemas informáticos y controladores integrados

Es el conjunto de posibles comunicaciones que se desarrollan en el ámbito digital a través de los diferentes dispositivos, canales y medios que permiten la interactividad entre usuarios

Algunas definiciones de Ciberespacio

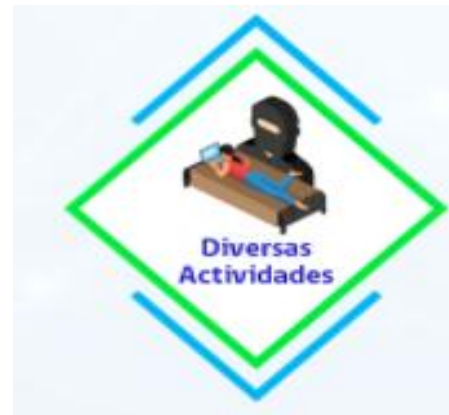


Han pasado más de 30 años de la novela “Neuromante”, pero no deja de llamar la atención el cómo esa idea de Ciberespacio se hace cada vez más propia.

Con esto, podemos hacernos las siguientes preguntas:

- ¿Cuál es la importancia del Ciberespacio para nosotros?
- ¿Cómo podemos enterarnos de novedades o de acontecimientos en la actualidad?

Algunas características del Ciberespacio



Introducción a la Ciberseguridad

¿Qué es la Ciberseguridad?

La Ciberseguridad es el mínimo de riesgos para el ciberespacio en lo referente a la protección de la confidencialidad, integridad y disponibilidad de la información.



La Ciberseguridad está compuesta por la capacidad de resistir, contener y recuperarse rápida y eficazmente después de un evento que atenta contra la Seguridad de la Información, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos tecnológicos, sistemas y la información de una persona o institución.

Ámbito de la Ciberseguridad



- En este aspecto debemos ver que la Ciberseguridad está en todos lados, ya que estamos expuestos a riesgos con el sólo hecho de estar conectados a Internet.
- Si bien, el Internet es una fuente fabulosa de inagotable información, también nos expone a riesgos constantemente, los cuales nos pueden afectar negativamente, por supuesto, debido a que podemos perder la privacidad y confidencialidad de nuestros datos o, simplemente podemos ser víctima de robo de datos, estafas, fraudes, entre otros.

Algunos ejemplos de los “incidentes” más conocidos



Para saber un poco más...

Concepto	Definición
Spam	Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.
Malware	Programa malicioso que busca realizar daños en un sistema informático.
Spyware	Programa malicioso que espía y recopila información de un computador o dispositivo para luego enviarla a alguien externo.
Troyano	Es un Malware que puede parecer legítimo, pero al ejecutarlo puede tomar el control de nuestras computadoras de diferentes maneras.
<u>Exploit</u>	Significa explotar o aprovechar una vulnerabilidad de un sistema.
<u>Bot</u>	Programa informático que realiza acciones o tareas mecanizadas y repetitivas.
<u>DoS</u> / <u>DDoS</u>	DoS corresponde a un ataque desde una única IP u ordenador, mientras que <u>DDoS</u> corresponde a un ataque desde distintas IP u ordenadores.

Algunos consejos de Ciberseguridad...

El autocuidado es el elemento clave de la Ciberseguridad, ya que, si no nos protegemos, somos el eslabón más débil de la cadena, sin embargo, si aprendemos a cuidarnos adecuadamente, podemos ser la primera barrera de defensa ante ataques, incidentes, amenazas, entre otros.

Proteger puestos de trabajo; no dejar expuesta información sensible y bloquear computador al no utilizarlo

Las contraseñas deben ser secretas y únicas. Evitar anotarlas, compartirlas y reutilizarlas. Usar contraseñas de 14 caracteres, alfanuméricas, que incluyan símbolos.

Usar correo de forma segura. Utilizar redes sociales con perfil privado. No aceptar conexiones con desconocidos.

No pinchar enlaces sospechosos y reportar cuando se sospeche de un correo.

Nunca usar las mismas credenciales para aplicaciones y sitios web personales.

No transportar información sensible en medios removibles. Cifrar la información. Usar la nube.



Vulnerabilidades y amenazas

Vulnerabilidades y amenazas

Considerando que el Ciberespacio es un ecosistema dinámico y comprendiendo la importancia que tiene la Seguridad de la Información, debemos pensar qué motivos nos llevan a implementar medida preventivas y reactivas para asegurar la información.



En el Ciberespacio, así como en el mundo real, nos encontraremos constantemente con amenazas y con diferentes vulnerabilidades en torno a la información y su seguridad.

Vulnerabilidades

Una vulnerabilidad es vista como una debilidad en los procesos de tratamiento de información y, por tanto, podría afectar la seguridad de un sistema de información.



Las vulnerabilidades presentes en un sistema pueden ser explotadas por accidente o intencionalmente para tener acceso indebido y no autorizado a información, dando así un entorno ideal para la conformación de amenazas a los sistemas de información.

¿Qué hacer ante ellas?



Amenazas

Una amenaza consiste en aprovecharse de una manera intencionada de una vulnerabilidad de un sistema, con el objetivo de realizar acciones en contra de la seguridad y diferentes elementos de un sistema de información



De acuerdo al Instituto Nacional de Estándares y Tecnologías (NIST) “Las amenazas de seguridad cibernética explotan la mayor complejidad y conectividad de los sistemas de infraestructura crítica, lo que pone en riesgo la seguridad de la nación, su economía, la salud y seguridad pública”.

Características de las amenazas



Ciberamenazas

¿Qué es una Ciberamenaza?

Se pueden definir como aquellas acciones causadas por terceros con la intención de causar algún tipo de daño dentro del Ciberespacio.

De acuerdo a la Interpol, “las ciberamenazas evolucionan sin cesar, adaptándose a las conductas de los usuarios y las tendencias en línea para sacar partido de ellas”, asegurando, además, que media humanidad está en peligro y por tanto a ser víctima de la ciberdelincuencia a través de uno o más de los seis principales ciberataques:

- Phishing.
- Malware.
- Ransomware.
- Extorsión sexual.
- Minería ilícita de criptomonedas.
- Estafa a empresas por correo, mediante suplantación de identidad.
- Delitos en línea contra menores (Grooming).



Ciberamenazas más comunes



Phishing

¿Qué es el phishing?

Es la acción realizada por ciberdelincuentes que buscan, mediante diferentes técnicas de engaño, que una posible víctima comparta información sensible, tales como contraseñas y números de tarjetas de crédito.

- **¿Cómo funciona el phishing?**

- Generalmente la información que contiene el phishing viene con intención de infundir preocupación en la víctima, como por ejemplo una multa inexistente y exigiéndole visitar un enlace que lo llevará al robo de sus datos.

- **¿Cómo identificar el phishing?**

- La técnica más común es mediante el envío de correos electrónicos o mensajes que suplantan a una organización o persona de confianza de la víctima.

- **¿Cómo evitar el phishing?**

- No abrir enlaces que puedan parecer sospechosos. Es importante verificar que el remitente sea realmente quién dice ser, por ejemplo, viendo su dirección de correo o número.

Malware

¿Qué es el malware?

- Es el término que se usa para definir al software malicioso que busca causar daño a las personas, a la información y los diferentes dispositivos sin el consentimiento de los usuarios.

• ¿Cómo funciona el malware?

- El malware funciona con la descarga voluntaria o involuntaria del archivo por parte del usuario. Una vez dentro del dispositivo puede funcionar en segundo plano y borrar información que pueda ser sensible.

• ¿Cómo identificar el malware?

- Los diferentes tipos de malware suelen presentarse como archivos compartidos o en mails, descargas o dispositivos USB. En los dispositivos suelen verse ventanas emergentes, ralentización del equipo y falta de información y datos del usuario.

• ¿Cómo evitar el malware?

- No acceder a enlaces o descargas sospechosas. Una de las formas más eficientes de identificarlos es hacer un análisis preventivo a la información con algún antivirus.

Ransomware

¿Qué es el ransomware?

- Es un malware que impide a los usuarios acceder a su información y exigiendo un pago de rescate de la información frente al secuestro de datos.
- **¿Cómo funciona el ransomware?**
 - Funciona en base a la ingeniería social y, al igual que el phishing, con la intención de infundir temor en la víctima. Esto es con la intención de que la víctima se sienta presionada a pagar por una suma de dinero por liberar su información.
- **¿Cómo identificar el ransomware?**
 - Suele venir en correos no deseados. En la mayoría de los casos el mensaje contiene un archivo adjunto que parece ser legítimo, como un PDF, Excel u otro que contenga el ransomware.
- **¿Cómo evitar el ransomware?**
 - No descargar archivos adjuntos de correos que parezcan ser sospechosos, ya que podríamos ser víctimas de algún tipo de extorsión. También es recomendable escanear nuestros correos en búsqueda de malware.

DoS/DDoS

¿Qué son los ataques DoS/DDoS?

- DoS corresponde a un ataque desde una única IP u computador, mientras que DDoS corresponde a un ataque desde distintas Ips u computadores. Esto con el fin de exceder el límite de capacidad del sistema y evitar su correcto funcionamiento.
- **¿Cómo funcionan los ataques DoS/DDoS?**
 - Funciona enviando gran cantidad de solicitudes a un servidor, provocando la saturación del mismo y la caída o no disponibilidad de sus servicios y acceso a la información.
- **¿Cómo identificar los ataques DoS/DDoS?**
 - Se debe realizar un análisis en la latencia del servicio. También mediante la identificación de usuarios potencialmente sospechosos.
- **¿Cómo evitar los ataques DoS/DDoS?**
 - A través de la creación y la correcta configuración de un firewall para poder monitorear el tráfico en el servicio. Además de mantener seguros los equipos de trabajo y tomar medidas de prevención frente a los primeros indicios de ataque.

Ciberamenazas del siglo XXI

Hackers

En el lenguaje colectivo suele usarse el concepto de hacker para definir o identificar a una persona que tiene grandes habilidades informáticas y realiza ciberataques, siendo relacionado a la idea de un pirata informático, sin embargo, es importante precisar que un hacker es una persona que investiga un sistema informático, aplicación, entre otras, para buscar vulnerabilidades, reportarlas y desarrollar técnicas de mejora.



Ciberdelincuente

- Si bien, posee las mismas habilidades de un hacker, como el encontrar vulnerabilidades o fallas sistemas, aplicaciones, entre otros, los ciberdelinquentes suelen usarlas para realizar actividades ilícitas como el robo de información, estafas, sabotaje informático, phishing, entre otros.
- Los objetivos de los ciberdelinquentes son variados, ya que pueden atacar a personas, empresas, organizaciones y gobiernos.
- Si bien, en el lenguaje común suele interpretarse como “hacker”, lo cierto es que el concepto apropiado sería “cracker” o “ciberdelincuente”, ya que suelen desarrollar, por ejemplo, virus para introducirse en sistemas informáticos de forma ilícita y destruirlos.

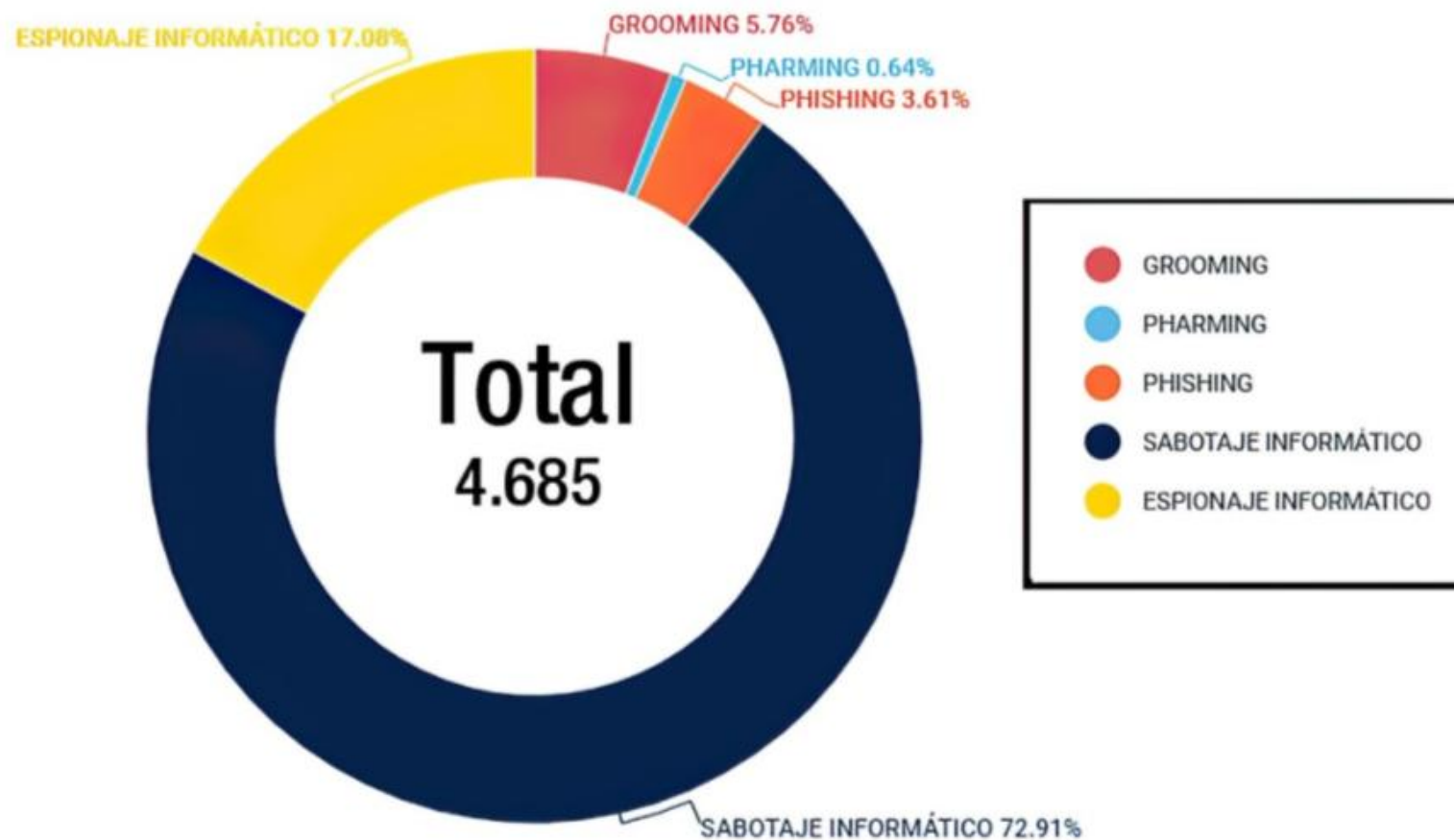


Ciberdelito / Cibercrimen

De acuerdo al 13° Congreso sobre Prevención del Delito y Justicia Penal del año 2015, un ciberdelito es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet. En tanto, en nuestra legislación, de acuerdo a la Ley n°21.459, son delitos tipificados:

- Ataque a la integridad de un sistema informático.
- Acceso ilícito.
- Interceptación ilícita.
- Ataque a la integridad de datos.
- Falsificación informática.
- Recepción de datos informáticos.
- Fraude informático.
- Abuso de dispositivos.

Cibercrímenes más comunes



Fuente:

<https://www.pdichile.cl/centro-de-prensa/detalle-prensa/2019/07/10/panorama-de-las-denuncias-en-ciberdelito>

Pharming

Es un ciberataque que consiste en redirigir el tráfico de una web al sitio del atacante, el que generalmente es un sitio fraudulento similar al original, con el objetivo de robar información personal. Esto se logra explotando las vulnerabilidades de software en los sistemas de nombre de dominio o DNS. Se usa comúnmente para simular sitios de entidades bancarias o gubernamentales, donde pedirán datos personal, lo que podría conllevar a un eventual phishing



¿Cómo prevenir el Pharming?

- Evitando sitios web que puedan parecer sospechosos, ya sea en errores de diseño u ortográficos en su web.
- Revisar que las páginas sean seguras y comiencen con `https://`



Vishing

El concepto viene de Voice y Phishing.

El engaño consiste en llamadas telefónicas simulando ser un servicio que usa la víctima, como por ejemplo el banco. Mediante estas técnicas buscan obtener datos personales como pueden ser las terceras claves, token de validación, entre otros.



Smishing

El concepto viene de SMS y Phishing.

El engaño consiste en enviar mensajes de texto o mensajería instantánea simulando ser un servicio que utiliza la víctima. Al igual que el phishing, suele contener enlaces que redirigirán a la víctima a un sitio fraudulento, donde le pedirán ingresar sus datos de acceso.



Cryptojacking

El Cryptojacking es la minería ilícita de criptomonedas y ha sabido aprovechar su auge durante los últimos años. El atacante puede hacer uso de un malware o incluso de sitios web fraudulentos para instalar aplicaciones que toman el control de los equipos y destinan los recursos del hardware, tales como el uso de CPU para la minería ilícita, afectando considerablemente el rendimiento de los equipos informáticos.



¿Cómo prevenir el Cryptojacking?

Usando extensiones de navegador para bloquear minería de criptomonedas.

Revisando constantemente el uso de recursos de nuestro equipo, considerando el rendimiento y temperatura del equipo.

.

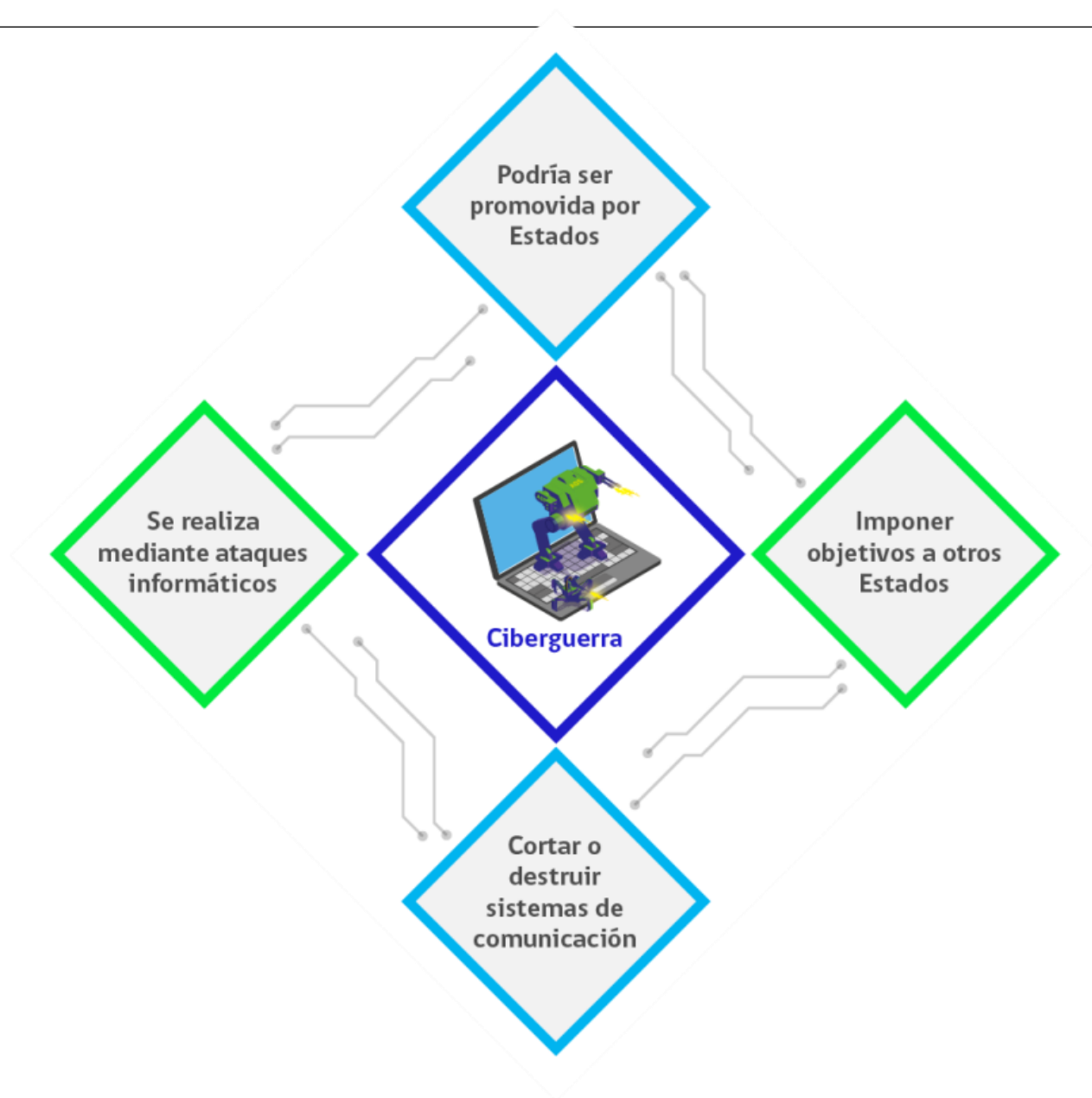


Ciberguerra

En los tiempos actuales y venideros, las trincheras podrían cambiar. De momento no ha estallado una ciberguerra en el mundo, pero las nuevas tecnologías y el valor de la información podrían promoverla. Una definición de ciberguerra plantea que: “puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física, sino que un ataque informático.”

Fuente: Los estados y la Ciberguerra, Gema Sánchez Medero.

Ciberguerra



Ciberterrorismo

Tanto el ciberterrorismo como el concepto de terrorismo están en constante definición. Una de ellas apunta a que podría entenderse como aquellas acciones que mediante el uso de tecnologías de la información y la comunicación busquen generar o infundir el miedo y terror en una población.



Hacktivismo

Son actos que apuntan a diferentes ramas, como puede ser la política, libertad de expresión, derechos, democratización y ética de la información, entre otros. El factor común es el activismo que puedan desarrollar, pero en el contexto del ciberespacio. El hacktivismo destaca por los ataques DoS y defacements, que consiste en la acción de entrar sin autorización en un servidor y modificar la página principal dejando algún mensaje.



Hacktivismo

