SEGUROS COMERCIALES BOLÍVAR

GLOSARIO

¡TODO LO QUE NECESITAS SABER SOBRE

EVOLUCIONA

con Ciberseguridad Pymes

- **Amenaza (informática):** Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial de efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus) [1]

- **Ciberataque:** Es la explotación deliberada de sistemas informáticos, empresas y redes dependientes de la tecnología. Estos ataques utilizan códigos maliciosos para alterar la lógica o los datos del ordenador, lo que genera consecuencias perjudiciales que pueden comprometer información y provocar delitos cibernéticos, como el robo de identidad. [2]

- **Cibercriminal:** Es la persona que planea y/o ejecuta el ciberataque aprovechando una vulnerabilidad en el sistema mediante el engaño a personas.

- **Ciberseguridad:** Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual. [3]

- **Cobertura ciberseguridad Pymes:** Es un anexo que la Pyme contrata para protegerse de un ciberataque. Cuentan con un plan de protección básico o full según la necesidad del cliente. Este anexo hace parte de la póliza de Tranquilidad Pymes.

- **DoS o denegación de servicio:** Es saturar de tráfico un sitio web, sobrecargando su servidor para que le sea imposible publicar su contenido a los visitantes. Aunque esto puede ocurrir porque el enlace de una noticia masiva se haya roto; a menudo es provocado con fines maliciosos.[4]

---

1. *https://www.incibe.es/protege-tu-empresa*
2. *Camara de Valencia. Tecnología para los negocios. https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/*
3. *Oxford Languages. https://languages.oup.com/google-dictionary-es/*
4. *Idem.*

- **Errores operativos:** Una acción, un concepto o una cosa que no se realizó de manera correcta.[5]

- **Hacker:** Persona con grandes conocimientos de informática que se dedica a detectar fallos de seguridad en sistemas informáticos.[6] No todos los hackers son cibercriminales.

- **Malware:** Son varias formas de software dañinos o códigos dañinos, como son los virus o los ransomware. Una vez que entra en el ordenador, puede causar todo tipo de estragos, desde tomar el control de la máquina y monitorear las acciones y pulsaciones de teclas, hasta enviar silenciosamente todo tipo de datos confidenciales a la base de origen del atacante.[7]

  Ejemplo: El conocido virus Troyano (es un componente de malware que puede dañar, robar o de algún otro modo damnificar los datos en su red de ordenadores. A menudo llamados Troyanos a secas, este software malicioso normalmente está disfrazado de programa de ordenador legítimo).[8]

- **Phishing:** Es la suplantación de identidad, suele ser la principal vía que utilizan. Para combatir este tipo de ataques, es esencial comprender la importancia de verificar los remitentes de correo electrónico los archivos adjuntos y enlaces.[9]

- **Ransomware:** Es un programa de software malicioso que infecta la computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema. Este tipo de malware es un sistema criminal para ganar dinero, se puede instalar a través de enlaces engañosos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web. El ransomware tiene la capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña.[10]

- **Seguridad Informática:** Es el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica proteger el uso de los recursos informáticos contra intrusos que pueden tener intenciones maliciosas de obtener ganancias o incluso la posibilidad de acceder a ellos por accidente.[11]

---

5. Definición.de
6. Idem. Oxford Languages.
7. Idem.
8. https://softwarelab.org/es/que-es-un-troyano-informatico/
9. Idem
10. ¿Qué es el Ransomware?
https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware
11. Universidad Internacional de Valencia. Qué es seguridad informática. https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

- **Vulnerabilidad (informática):** Es una debilidad o fallo en un sistema digital que pone en riesgo la seguridad de la información, permitiendo que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.[12]

- **Virus informático:** Es un programa o código malicioso y autorreplicante que se cuela en su dispositivo sin su conocimiento ni permiso.[13] Es un tipo de malware.

SEGUROS COMERCIALES BOLÍVAR

12. *https://www.incibe.es/protege-tu-empresa*
13. *Avast https://www.avast.com/es-es/c-computer-virus*