



**UNIVERSIDAD AUTÓNOMA DE CHIRIQUÍ
FACULTAD DE ECONOMÍA
ESCUELA DE CIENCIAS COMPUTACIONALES
LICENCIATURA EN GESTIÓN DE LAS TECNOLOGÍAS**

**MATERIA:
PROYECTOS DE TECNOLOGÍA DE INFORMACIÓN**

**TRABAJO:
INVESTIGACIÓN #1**

**ESTUDIANTE:
JUAN ANTONIO GARCÍA GARCÍA CÉD: 4-782-2173**


**PROFESOR:
ANDRÉS MIRANDA**

2024

INVESTIGACIÓN N°1


Instrucciones: Busque el significado, ilustre con imágenes y ejemplifique cada uno de ellos.

1. ¿Qué es?

 **Seguridad:** Estado de ausencia de vulnerabilidades, amenazas o riesgos debido al establecimiento de medidas y políticas de seguridad para la protección de los bienes informáticos en cualquier red, sistema o equipo computacional que posee una organización.


Ejemplo: Implementación de un antivirus en un ordenador para la detección de virus.



 **Contingencia:** Estrategia planificada o medidas, constituidas por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación encaminados a conseguir una restauración progresiva y ágil de los servicios computacionales de una organización, afectados por una paralización total o parcial de la capacidad operativa, cuyo fin fundamental es el de minimizar los tiempos y costos asociados con interrupciones no planeadas del servicio de computación.


Ejemplo: Planificación para la implementación de almacenamiento en la nube o servidor, lo cual permitiría la recuperación de datos en caso de robos, borrado o daño a nivel físico de los equipos tecnológicos.



 **Amenazas:** Una amenaza de ciberseguridad se refiere a cualquier situación o caso que pueda tener consecuencias negativas como la obtención de acceso no autorizado o explotar cualquier vulnerabilidad del sistema de información, y comprometer así su confidencialidad, integridad o disponibilidad afectando las operaciones, funciones, marca, reputación o imagen percibida de una empresa.



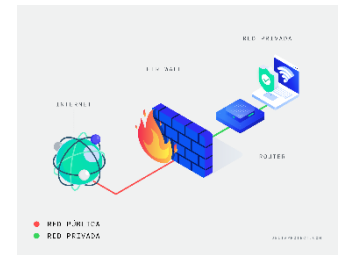
Ejemplo: Descarga de archivos por parte de usuarios de la empresa y que al ejecutarse se realicen ciertas actividades en segundo plano o ejecuten comandos que borren o extraigan datos importantes.

 **Riesgos:** Son posibles amenazas, vulnerabilidades o debilidades en los sistemas, redes, aplicaciones y datos de una organización que podrían ser explotados por atacantes. Generalmente se puede catalogar un riesgo como aquella incertidumbre existente por la posible realización de un suceso relacionado con la amenaza o daño respecto a los bienes o servicios informáticos.

Ejemplo: Al crear un entorno para compartir archivos mediante el servidor Samba el puerto 445, puede ser riesgoso si no se cuenta con actualizaciones o parches de seguridad, de lo contrario los atacantes pueden acceder de manera remota a los sistemas e infectarlos.



Firewall: Es un elemento informático que controla el tráfico entrante y saliente de un dispositivo o una red privada con la finalidad de bloquear la entrada de datos que no cumplan con algunos criterios de seguridad, es decir que evita intrusiones de usuarios no autorizados y de data maliciosa que pueda dañar los sistemas o dispositivos conectados a una red de acceso local con el objetivo de proteger los datos.



Ejemplo: La implementación o creación de reglas de firewall es un practico ejemplo de como se pueden bloquear puertos, acceso al sistema y protección en la transmisión de datos.

Seguridad informática: Es el conjunto de tecnologías, procesos y prácticas diseñadas para la protección de redes, dispositivos, programas y datos en caso de algún ciberataque, hackeo, daño o acceso no autorizado, es decir que va más allá de programas o detectores de software malicioso, ya que no solo debe salvaguardar la integridad de los dispositivos, sino garantizar la privacidad y la información que pueda almacenar, enviar o recibir entre dispositivos.



Ejemplo: Aplicación de las ISO 9000 y 27000 para mejorar la seguridad de la red, equipos y apoyarse para la creación de políticas de seguridad.

2. Mencione tres consideraciones de aplicar Antivirus en su computadora, ejemplifique

1. Sistema operativo: Existen múltiples sistemas operativos como Windows, MAC, Linux y no todos los antivirus funcionan para cualquiera de ellos. Por eso, se debe tener en cuenta que si se desea una protección integral es necesario saber las características o funcionalidades que presta el antivirus para el sistema operativo que se posee.

Ejemplo: Antes de adquirir un antivirus se debe realizar un estudio del ordenador y de su sistema, tanto para conocer su capacidad de soporte, como su necesidad específica.

2. Información: El tipo de información es uno de los aspectos más importantes a la hora de plantearse la aplicación de un antivirus, saber el tipo de usabilidad que le

damos a nuestro computador o el tipo de información que se maneja, puede orientarnos a encontrar un antivirus que cumpla con las necesidades de protección correspondientes.

Ejemplo: Si se realizan transacciones en línea, lo más correcto es instalar un antivirus que mantenga a salvo la información que brindas al realizar estas operaciones, para que no sea robada o utilizada por terceros.

- 3. Detección de malware:** Dado que el trabajo del software antivirus es detectar amenazas, debe funcionar sin problemas, por lo tanto es necesario asegurarse de que el software antivirus pueda bloquear más del 95% del malware, ya sea malware común o nuevo y que su tasa de detección no esté acompañada de una alta tasa de falsos positivos, que es cuando los archivos benignos se confunden con malware.

Ejemplo: Si se descargan archivos constantes es ideal que el antivirus analice los archivos en busca de virus o cualquier agente malicioso dentro de los archivos.

3. ¿Cuál es el objetivo principal de aplicar Seguridad Informática en las Empresas?

R: El objetivo principal de la aplicación de seguridad informática en una empresa se basa en la protección de los datos, lo cual representa un valor económico muy importante para la organización. El cumplimiento de este objetivo se logra mediante la aplicación de buenas prácticas y defensas esenciales para evitar amenazas, riesgos y vulnerabilidades que puedan presentar los equipos tecnológicos frente a ataques cibernéticos o violaciones de datos, por lo tanto se aplica seguridad informática con la intención de mantener a raya tanto las amenazas internas y externas buscando que la información que se posee siempre esté segura, confiable, disponible e íntegra para aquellos que la manipulan o tratan.

Ejemplo: Un claro ejemplo de la aplicación de Seguridad Informática son los bancos, pues estos necesitan proteger un sinnúmero de datos, como transacciones, datos de clientes, datos de empleados, datos bancarios, así mismo como la red en la que trabajan.

4. Mencione tres Políticas de Seguridad, dos ventajas y dos desventajas.

EQUIPOS

De la Instalación de Equipo de Cómputo.

1. Todo el equipo de cómputo (computadoras, estaciones de trabajo, servidores, y equipo accesorio), que esté o sea conectado a la red de la empresa, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe sujetarse a las normas y procedimientos de instalación que emite el departamento de SOPORTE TECNOLÓGICO E INFORMÁTICO.

Del Mantenimiento de Equipo de Cómputo.

2. La oficina de SOPORTE TECNOLÓGICO E INFORMATICO, corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar.

DEL CONTROL DE ACCESOS

Del Acceso al equipo de cómputo.

3. Las áreas de cómputo de los departamentos donde se encuentre equipo cuyo propósito reúna características de imprescindible y de misión crítica, deberán sujetarse también a las normas que establezca oficina de SOPORTE TECNOLÓGICO E INFORMATICO.

Ventajas de las Políticas de Seguridad.

- **Protección de datos sensibles:** Ya que las empresas manejan una gran cantidad de datos sensibles, como información financiera, datos de clientes y empleados, propiedad intelectual y estrategias comerciales, entre otros, las políticas de seguridad informática establecen medidas para proteger estos datos y evitar su acceso no autorizado, robo o filtración.
- **Prevención de brechas de seguridad:** Las brechas de seguridad pueden resultar en pérdidas de datos, interrupción de servicios, daños a la reputación y pérdida financiera. En este sentido, las políticas de seguridad informática establecen prácticas y controles para prevenir y mitigar las brechas de seguridad, como el uso de contraseñas seguras, la implementación de firewalls y el cifrado de datos.

Desventajas de las Políticas de Seguridad.

- **Vulnerabilidades por configuraciones inadecuadas:** Si los sistemas de seguridad no están configurados correctamente, pueden dejar vulnerabilidades, riesgos o generar un falso sentido de seguridad en cualquier dispositivo o red perteneciente a la organización.
- **Exceso de confianza y desactualización:** A veces, las organizaciones pueden confiar excesivamente en sus políticas de seguridad que muchas veces suelen estar obsoletas frente a nuevas brechas de seguridad, lo que las lleva a descuidar otras medidas de protección o a subestimar las amenazas emergentes provocando pérdidas de gran valor.

Conclusiones

- La aplicación de Seguridad Informática es unos aspectos más importantes que deben considerar las organizaciones para evitar pérdidas de datos, costos innecesarios y demandas.

- ✚ Toda vulnerabilidad o amenaza debe ser detectada a tiempo por los expertos en seguridad informática para que se realicen los ajustes necesarios, se actualicen componentes o se apliquen parches adecuados con el objetivo de disminuir situaciones peligrosas para la organización en un 0%.
- ✚ Las Políticas de seguridad son muy importantes y necesarias para un correcto funcionamiento de los equipos o para que quienes los administren sean conscientes de que su cumplimiento es vital tanto para la empresa como para el usuario.