UNIVERISDAD AUTONOMA DE CHIRIQUI
FACULTDAD DE ECONOMIA
LICENCIATURA EN GESTION DE TECNOLOGIAS DE INFORMACION

SEGUIRIDAD INFORMATICA

PROFESOR ANDRES MIRANDA

INVESTIGACION

Jesús Noel Del Cid 4-746-1085

1. **Seguridad**: Es la capacidad de dar respuesta efectiva a riesgos, amenazas o vulnerabilidades y estar preparados para prevenirlos, contenerlos y enfrentarlos.
   Ejemplo: Seguridad de 2 pasos

2. **Informática:** La informática, también llamada computación, es el área de la ciencia que se encarga de estudiar la administración de métodos, técnicas y procesos con el fin de almacenar, procesar, transmitir información y datos en formato digital.
   Ejemplo: Uso de sistemas de ofimática

3. **Normas de seguridad:** conjunto de directrices que mantienen el control de la confidencialidad de la información, aseguran la correcta operación de los equipos y sistemas de una empresa.
   Ejemplo: Prohibir el uso de memorias USB en los equipos de la empresa.

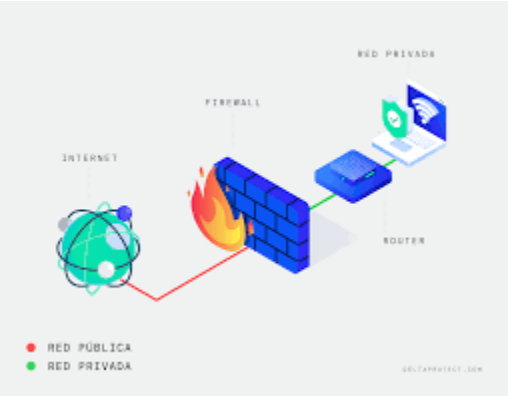
4. **Contingencia:** En términos informáticos un plan de contingencia es un programa alternativo para que una organización pueda recuperarse de un desastre informático y restablecer sus operaciones con rapidez.
   Ejemplo: uso de sistemas de respaldo de datos.

5. **Amenazas:** Una amenaza es una posible acción o evento negativo habilitado por una vulnerabilidad que resulta en un impacto no deseado en un sistema o aplicación informática. También puede referirse a un incidente nuevo o recién descubierto que tiene el potencial de dañar un sistema o su empresa

en general, es una forma común en que los piratas informáticos hacen su movimiento.
Ejemplo: un ataque tipo ransomware

6. **Riesgos:** Es la posibilidad de vulnerabilidades y amenazas a los que se encuentran expuestos los sistemas informáticos o probabilidad de la ocurrencia catástrofe causando daños o pérdida a la información o recursos.
Ejemplo: un incendio, un ataque informatico.

7. **Firewall:** Es un sistema de seguridad de red de las computadoras que restringe el tráfico de internet entrante, saliente o dentro de una red privada. Este software o esta unidad de hardware y software dedicados funciona bloqueando o permitiendo los paquetes de datos de forma selectiva. Se utilizan con frecuencia para evitar que otros usuarios tengan acceso a las redes privadas conectadas a internet.
Ejemplo: Firewall de Windows, hardware: FortiGate



8. **Seguridad informática:** La seguridad de la tecnología de la información (seguridad informática) constituye un amplio conjunto de medidas multidisciplinares diseñadas para proteger la integridad, confidencialidad, disponibilidad de la información y sistemas, con el fin de evitar que una red informática y sus datos sufran algún tipo de vulneración, filtración, publicación de información privada o ataque.
   Ejemplo: el uso de contraseñas ligado al con un número celular o correo electrónico para controlar el acceso.

Mencione 3 consideraciones de aplicar un Antivirus en su computadora

1. La selección de un antivirus para mi computadora seria uno de acorde a los recursos con los que cuenta mi ordenador. En este sentido para mí concepto el Windows Defender hace buen trabajo ya que al estar integrado con Windows el impacto en el sistema es bajo y su coste pues viene integrado con la licencia del propio sistema operativo

2. Otra consideración a tomar en cuenta sería el costo de la licencia o suscripción al servicio que permite recibir actualización de la base de dato de virus o definiciones de las mismas.

3. Capacidad de detección con el fin de escoger un buen antivirus de paga que no tenga un impacto negativo en el sistema, tendría que realizar un estudio de las características de los antivirus actuales para escoger uno que sea capaz de mantener mi equipo protegido.

¿Cuál es el objetivo principal de aplicar seguridad informática en las empresas?

El objetivo principal de aplicar seguridad informática en una empresa es la protección de la información con el fin de mantener la confidencialidad así como la integridad de los mismos evitando así la divulgación de información sensible de una empresa.

Mencione 3 políticas de seguridad 2 ventajas y desventajas

- Políticas de seguridad de contraseña.
- Política de acceso y privilegios.
- Política de uso aceptable.

Políticas de Seguridad de Contraseña

Ventajas:

1. **Mayor Protección contra Ataques**: Las políticas estrictas de contraseñas, como exigir combinaciones de letras, números y símbolos, ayudan a proteger las cuentas contra ataques de fuerza bruta y adivinación.
2. **Reducción de Riesgos Internos**: Una política que requiere la renovación periódica de contraseñas disminuye el riesgo de acceso no autorizado por parte de personas que puedan haber obtenido contraseñas antiguas.

Desventajas:

1. **Complicación para los Usuarios**: Reglas estrictas pueden llevar a contraseñas difíciles de recordar, lo que puede resultar en que los usuarios escriban sus contraseñas en lugares inseguros o usen métodos poco seguros para recordarlas.
2. **Posible Rechazo del Usuario**: Los usuarios pueden sentir que las políticas son demasiado severas y podrían intentar evadirlas usando contraseñas menos seguras o escribiéndolas en lugares inseguros.

Políticas de Acceso y Privilegios

Ventajas:

1. **Control de Acceso Eficiente**: Al definir claramente quién tiene acceso a qué recursos, estas políticas ayudan a asegurar que solo el personal autorizado pueda acceder a información sensible, reduciendo el riesgo de filtraciones.
2. **Cumplimiento Normativo**: Facilitan el cumplimiento de normativas y estándares de seguridad, al garantizar que los accesos estén bien documentados y justificados.

Desventajas:

1. **Gestión Compleja**: Puede ser complejo gestionar y mantener los permisos adecuados, especialmente en organizaciones grandes o en crecimiento. Los errores pueden llevar a accesos inapropiados o bloqueos innecesarios.
2. **Impacto en la Productividad**: Los procesos para solicitar y aprobar cambios en los accesos pueden ser lentos, lo que puede afectar la capacidad de los empleados para realizar su trabajo de manera eficiente si necesitan acceso inmediato.

Políticas de Uso Aceptable

Ventajas:

1. **Claridad en el Uso de Recursos**: Establecen reglas claras sobre cómo deben usarse los recursos tecnológicos, ayudando a prevenir el uso indebido y asegurando que los recursos se utilicen de manera productiva.
2. **Protección Legal**: Ofrecen una base legal para tomar medidas disciplinarias en caso de violaciones, protegiendo a la organización contra posibles abusos y asegurando un entorno de trabajo más seguro.

Desventajas:

1. **Restricciones en la Libertad del Usuario**: Pueden limitar la libertad de los empleados al restringir el acceso a ciertos sitios o aplicaciones, lo que puede afectar su satisfacción y moral si no se comunican claramente las razones de estas restricciones.
2. **Necesidad de Actualización Continua**: Las políticas de uso aceptable deben actualizarse regularmente para adaptarse a nuevas amenazas y tecnologías, lo cual puede ser un proceso laborioso y requerir una vigilancia constante.

CONCLUSIÓNES

La presente investigación ha cumplido el objetivo de refrescar conceptos básicos vistos durante los años de estudios en la carrera y al mismo tiempo nos ha puesto a pensar en las decisiones cotidianas acerca de la seguridad y riesgo al nos enfrentamos a diario en el uso de los sistemas de información.

El uso de y la elección de un antivirus y es de vital importancia para mantener los sistemas de información relativamente seguros esto llevado de la mano con el uso de las adecuada políticas de seguridad representan un pilar básico para la protección de la información.

El objetivo de toda empresa debe ser mantener segura la información mediante la prevención de riesgos al contar con planes de contingencia y la detección de posibles amenazas y vulnerabilidades.