UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA

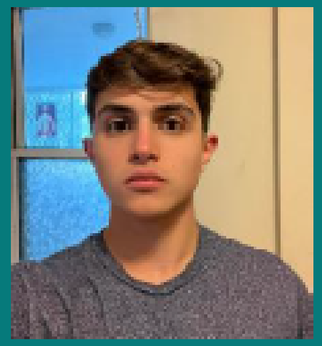
UNIDAD DE APRENDIZAJE: SISTEMAS OPERATIVOS

ACTIVIDAD FUNDAMENTAL 4
CATEDRÁTICO: DRA. NORMA EDITH MARIN MARTINEZ

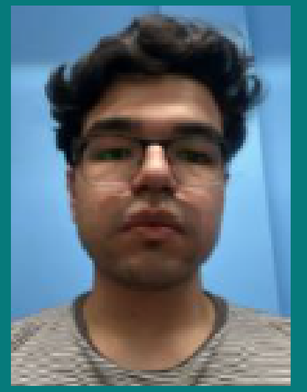
HORA: N4-N6 GRUPO: 004
EQUIPO 4

2010184 Andrea Ximena Rivera Aceves

2001403 Ricardo Rodríguez Lozano



2082321 Jesús Salvador Guzmán Hernández



índice

Introducción

Desde que tenemos uso de razón como especie, el humano ha hecho todo lo posible para salvaguardar la integridad de el mismo y de la gente que los rodea. Esto implica protegernos de amenazas externas para sobrevivir, y tambien proteger nuestra propiedad. Desde hace siglos que hemos implementado este tipos de medidas, en forma de muros, divisiones, llaves, contraseñas.

Esta practica no es ajena a los tiempos actuales; por lo contrario, ahora mas que nunca, con la llegada de los sistemas de información, se necesitan nuevos sistemas para protegernos de amenazas.

A continuación veremos más a detalle los sistemas de seguridad informática.

Back to Agenda Page

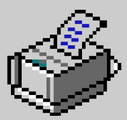
Redes y seguridad

Add a short description

11:11PM

Seguridad informática

La seguridad informática se encarga de prevenir y detectar el uso no autorizado de un sistema informático e implica la protección contra intrusos que pretendan utilizar las herramientas y/o datos empresariales maliciosamente o con intención de lucro ilegítimo.

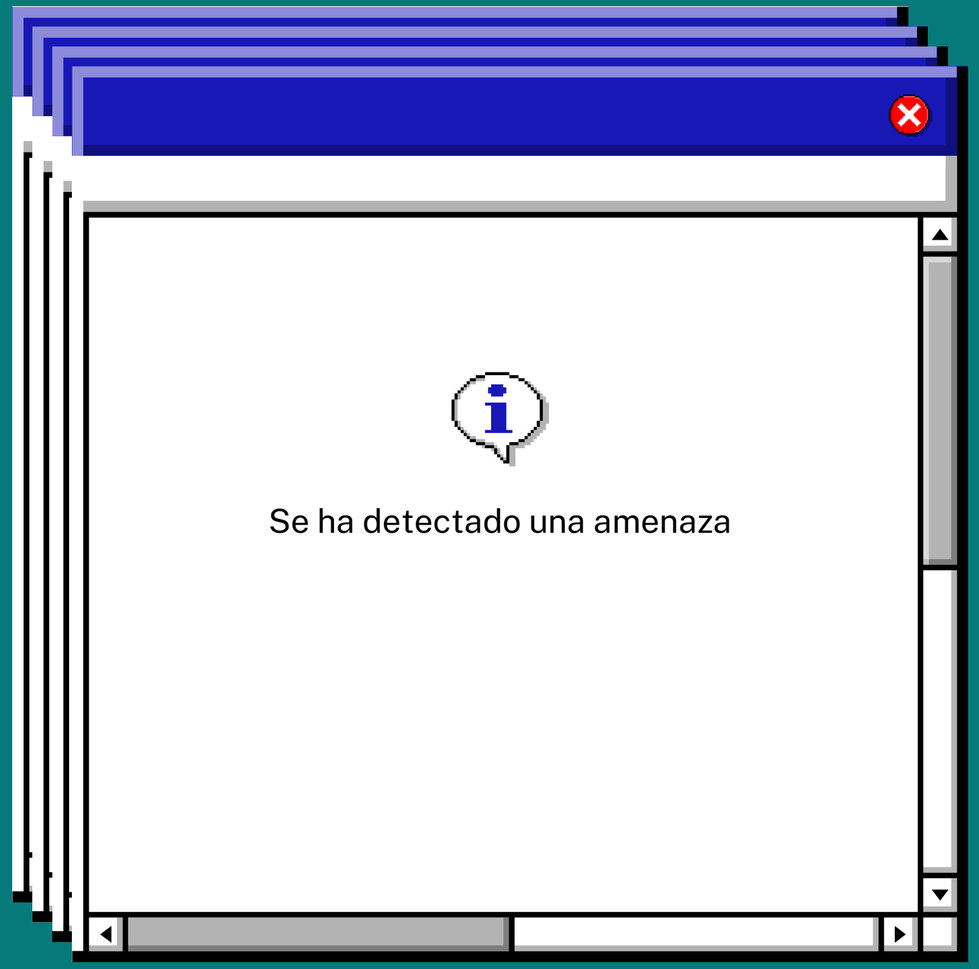





Back to Agenda Page

Amenazas cibernéticas

Existen varios tipos de amenazas cibernéticas, a continuación entraremos a detalle en las mas comunes:



Back to Agenda Page

Tipos de amenazas más comunes:

Malware

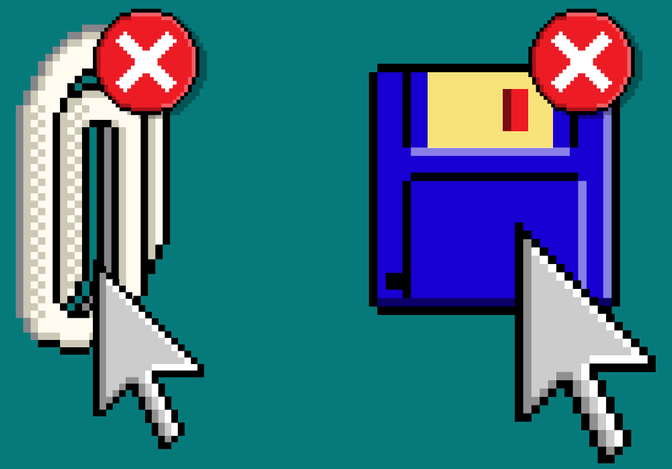
Phising

Inyeccion SQL

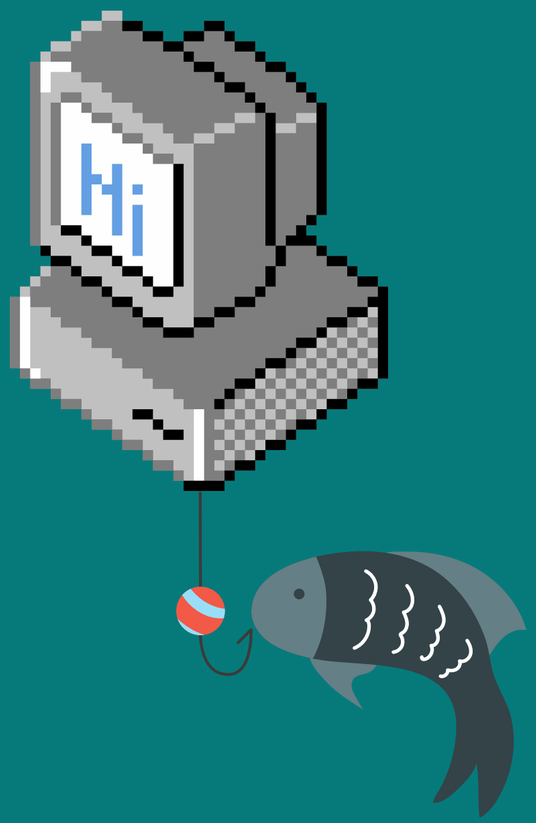
Back to Agenda Page

Malware

El malware es un tipo de software malicioso el cual se activa cuando el usuario hace clic sobre un link o algun archivo de dudosa procedencia. Un malware pueden ser distintos tipos de amenazas, desde un virus, un troyano o un gusano informatico; estos con el proposito de robar información o causar un daño al computador el usuario.



Back to Agenda Page



Phishing

El phishing se utiliza para obtener datos personales del usuario, en especial datos fiscales y bancarios, esto con el motivo de robar la información y robar dinero u otras cosas de valor para el usuario. Se tiene que tener un mayor cuidado con este tipo de amenazas ya que estan disfrazadas de correos u otro tipo de comunicaciones de supuestas empresas establecidas, pero que en realidad son interfaces falsas para obtener tu información personal

Back to Agenda Page

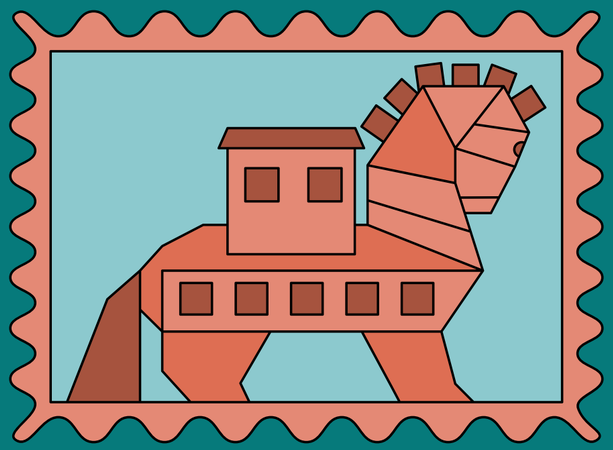
Inyección SQL

Esta amenaza es muy comun debido a su efectividad y el alcance que tiene el atque. Los ciberdelincuentes aprovechan las deficiencias de ciertos sistemas web para mandar su propio codigo y asi vulnerar la base de datos, esto con el fin de robar y/o alterar la base de datos. Pueden robar todo tipo de información de los usuarios dentro de esa base, desde correos, contraseñas, estados de cuenta, etc. Es comun que editen los saldos en las bases de datos financieras para asi transferirse dinero a sus propias cuentas.

Back to Agenda Page

Otras amenazas

Acabamos de ver las 3 amenazas mas utilizadas en el mundo, pero no por esto significa que sean las unicas, a continuación veremos otro tipo de amenazas



Troyanos

Es un tipo de malware que a menudo se disfraza de software legítimo. Los cibercriminales y hackers pueden utilizar troyanos para tratar de acceder a los sistemas de los usuarios. Una vez activados, los troyanos permiten a los cibercriminales espiarte, robar tu información confidencial y obtener acceso de puerta trasera a tu sistema.

Back to Agenda Page

Virus

En términos más técnicos, un virus informático es un tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo. Además, está diseñado para propagarse de un equipo a otro.

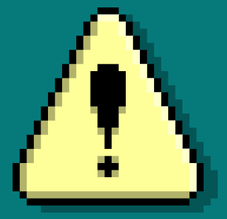
Spyware

Software malicioso que infecta el ordenador o dispositivo móvil y recopila información sobre el usuario, su navegación y su uso habitual de Internet, así como otros datos.

Back to Agenda Page

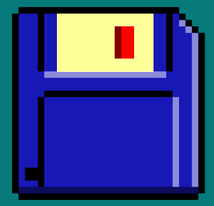
Análisis y prevencion de desastres

Back to Agenda Page



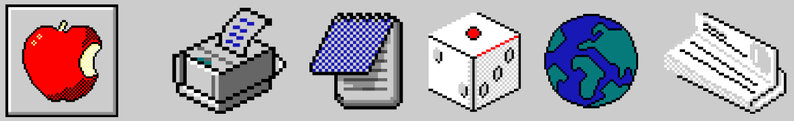
1. Controles de acceso a los datos más estrictos

¿Cómo proteger la información de una empresa? Una de las principales medidas de seguridad es limitar el acceso a la información. Cuantas menos personas accedan a una información, menor será el riesgo de comprometerla.



2. Realizar copias de seguridad

Poseer un sistema de copias de seguridad periódico permite que la empresa garantice que puede recuperar los datos ante una incidencia de carácter catastrófico, impidiendo la pérdida de los mismos y permitiendo la recuperación de la normalidad en el trabajo en apenas unos minutos.



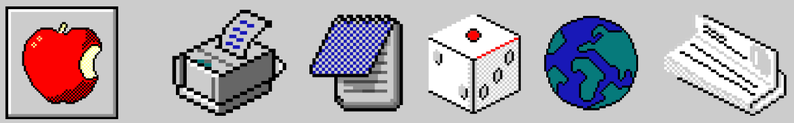
Back to Agenda Page

3. Utilizar contraseñas seguras

El acceso a las distintas plataformas que utiliza la empresa (correo electrónico, servidor de copias de seguridad NAS, etc.) debe realizarse utilizando claves de seguridad (contraseñas) seguras, que impidan que puedan ser fácilmente descubiertas por piratas informáticos.

4. Proteger el correo electrónico

Hoy en día, la mayoría de comunicaciones de nuestra empresa la realizamos utilizando el correo electrónico. Por lo tanto, otra medida de seguridad es utilizar filtros antispam y sistemas de encriptado de mensajes, para asegurar la protección y privacidad de toda esa información.



Back to Agenda Page

5. Contratar un software integral de seguridad

La mejor forma es contratando un paquete de seguridad integral que contenga antivirus, antiespías, antimalware, firewall, etc., y que permita proteger la información ante posibles ataques externos a través de internet.

6. Utilizar software DLP

Existen programas de prevención de pérdidas de datos (DLP) que pueden ser implementados como medida de seguridad en nuestra empresa para supervisar que ningún usuario esté copiando o compartiendo información o datos que no deberían.





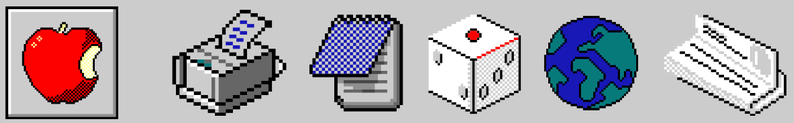

Back to Agenda Page

7. Trabajar en la nube

Trabajar en la nube permite, entre otras ventajas, contar con los sistemas de seguridad de la información que posee el proveedor de servicios. Además, este proveedor será responsable de esa seguridad.

8. Involucrar a toda la empresa en la seguridad

Para que las medidas de seguridad informática de una empresa funcione, debemos involucrar en su participación a todos los estamentos que participan en la misma, incluyendo a los agentes externos como puedan ser clientes, proveedores, etc. Muchas veces, nuestra empresa tiene implantados los sistemas correctos de seguridad, y la brecha en la misma, se produce al relacionarnos con un tercero que carece de estas medidas de seguridad.

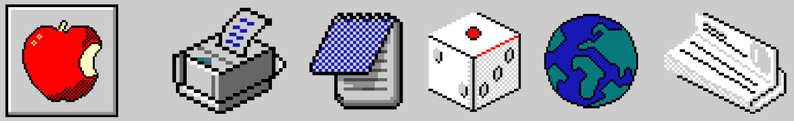


Back to Agenda Page

Administracion de riesgos y seguridad

La administración de riesgos es una pieza clave en la dirección de la empresa y se refiere a las gestiones que pretenden proteger y crear valor dentro de la empresa para lograr así alcanzar los objetivos y mejorar su efectividad.

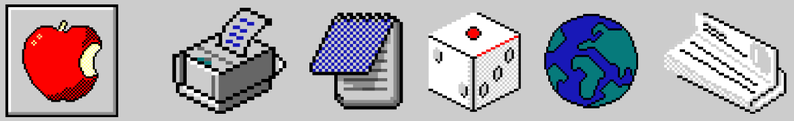
Es aquí en donde corresponde ejercer un control, inspección y vigilancia sobre la industria y los servicios de vigilancia y seguridad privada y llevar los procesos al pie de la letra para una mejora continua.



Back to Agenda Page

Soluciones en seguridad informatica

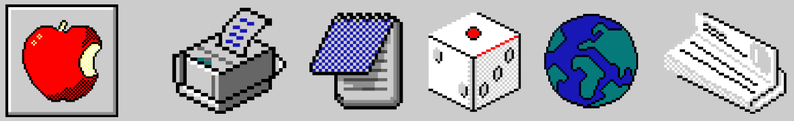
- Establecer normas para el uso preventivo de los dispositivos y plataformas a cumplir por el personal y sus usuarios.
- Crear un plan de acción que determine los pasos a seguir según las amenazas que podrían afectar a las empresa. Para ello se establecen las figuras a participar y su función según cada contingencia.
- Adquirir las herramientas necesarias que ayuden a prevenir dichas amenazas o en su defecto para protegerse de las mismas.



Back to Agenda Page

Soluciones en seguridad informatica

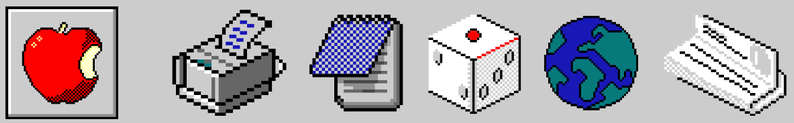
- Acordar con terceros (proveedores de servicios, software, técnicos) cuál será el plan a ejecutar en el caso de que ocurra una contingencia. De esta forma se puede conversar sobre la participación de cada uno, sin perjudicar a ninguno de los involucrados.
- Mantener un equipo experto en el tema o recurrir a especialistas que puedan asesorar o colaborar en este tema. Bien en su previsión o bien para solventar un problema.



Back to Agenda Page

Conclusión grupal

El análisis integral de la seguridad informática abarca la comprensión de diversas amenazas, como virus, malware, ransomware, entre otros. Además, se deben considerar distintos tipos de intrusos y autenticación, adaptándolos al contexto, ya sea para usuarios individuales, redes domésticas o empresas. La prevención de problemas y la gestión de riesgos son cruciales, junto con el mantenimiento de la seguridad de hardware y software. La elección de soluciones, como antivirus y firewalls, es vital, al igual que la educación del usuario. La seguridad informática es un proceso constante y adaptable a las cambiantes amenazas cibernéticas, con el objetivo de proteger datos e infraestructuras en un mundo cada vez más conectado.

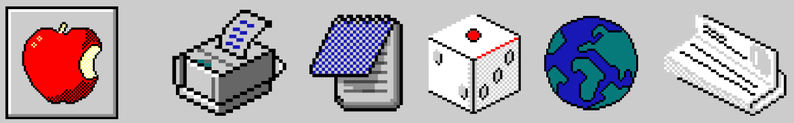


Back to Agenda Page

Conclusiones individuales

Andrea Ximena Rivera Aceves

En conclusión la seguridad informática se ha convertido en un factor fundamental en el entorno digital actual. Las amenazas cibernéticas, que abarcan desde virus y gusanos hasta malware y muchas otras formas de ataques, requieren un profundo entendimiento de las defensas necesarias. La autenticación y la seguridad son pilares fundamentales en la protección de la información y sistemas, tanto para usuarios individuales como para empresas y compañías de todos los tamaños. Por tanto, la seguridad informática no solo es esencial, sino que es un componente crítico para garantizar confianza y estabilidad en el mundo digital en constante evolución.



Back to Agenda Page

Jesús Salvador Guzmán Hernández

La seguridad informática es una prioridad para tanto empresa y personal, por ello es importante conocer este tema ya que en eso nos basamos en cómo podemos mejorar o planear algún filtro de seguridad que tengamos, como antivirus o algún sistema de firewall que nos ayude a contrarrestar estas amenazas, si no es posible esto, corremos riesgo en la información personal y empresarial, porque los ataques son para eso, afectar y atacar ala información que se tiene en el equipo

Ricardo Rodríguez Lozano

Actualmente la seguridad cibernetica es de suma importancia, en un mundo donde llevamos todos o la mayoria de nuestros movimeintos mediante el uso de la información, es vital que esta información no caiga en las manos equivocadas. Esto puede resultar en el robo de nuestra identidad, robo de dinero, extorsiones, entre otros males. Por eso es siempre bueno tener instaldo un buen antivirus y estar atento para no caer en amenazas, como lo puede ser el phishing de datos.

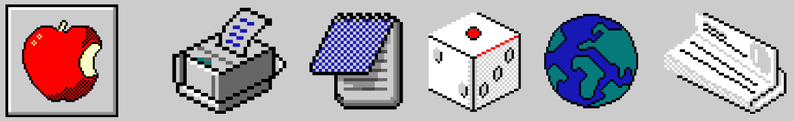
Referencias Bibliográficas

- Belcic, I. (2023, 25 junio). ¿Qué es el malware y cómo protegerse de los ataques? ¿Qué es el malware y cómo protegerse de los ataques? https://www.avast.com/es-es/c-malware#:~:text=Malware%20es%20un%20t%C3%A9rmino%20general,el%20sistema%20o%20robar%20datos.

- Tokio, R. (2023, 14 julio). ¿Cuáles son los principales tipos de amenazas informáticas? Tokio School. https://www.tokioschool.com/noticias/tipos-amenazas-informaticas/

- ¿Qué es la seguridad informática? | Glosario. (s. f.). HPE LAMERICA. https://www.hpe.com/lamerica/es/what-is/it-security.html#:~:text=La%20seguridad%20de%20la%20tecnolog%C3%ADa,de%20informaci%C3%B3n%20privada%20o%20ataque.

- Coppola, M. (2023, 8 mayo). Seguridad informática: qué es, tipos y características. Seguridad INFO. https://blog.hubspot.es/website/que-es-seguridad-informatica



Back to Agenda Page