



Guía de trabajo autónomo #7

Nombre del docente: Daniel Chaves Ureña

Taller Exploratorio: Tecnologías de la Información y la Comunicación

Unidad de estudio: Internet de todo y seguridad de los datos

Nivel: Décimo Año.

Horario de atención: A distancia lunes a viernes 7:00 a.m. – 4:30 p.m. (Según horario establecido)

Centro educativo: lunes a viernes 7:00 a.m. – 4:30 p.m. (Según horario establecido).

Escenario: 1 () 2 () 3 () 4 ()

Período establecido para el desarrollo de la guía:

II Parte. Planificación Pedagógica

Espacio físico, materiales o recursos didácticos que voy a necesitar: (Importante considerar la situación de cada uno de los estudiantes)	<ul style="list-style-type: none"> • Cuaderno de la subárea de Programación. • Lápiz o lapicero, según su preferencia, lápices de color de ser necesario. • Espacio cómodo, según la preferencia de cada estudiante y las posibilidades en el hogar o lugar de residencia.
Indicaciones generales:	Dicha GTA la encontraras en Microsoft Teams en el grupo de trabajo establecido para su respectiva sección, y en la Página del Colegio
Fecha de Entrega máxima:	8 de noviembre del 2021

Detalle de la planificación de las actividades que realiza el estudiante.

Resultado (s) de aprendizaje/Objetivo (s):

Marco teórico Internet de todo y seguridad de los datos

Ciberseguridad:

La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes

- La seguridad de red es la práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o malware oportunista.
- La seguridad de las aplicaciones se enfoca en mantener el software y los dispositivos libres de amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger. La seguridad eficaz comienza en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo.
- La seguridad de la información protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito.
- La seguridad operativa incluye los procesos y decisiones para manejar y proteger los recursos de datos. Los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría.
- La recuperación ante desastres y la continuidad del negocio definen la forma en que una organización responde a un incidente de ciberseguridad o a cualquier otro evento que cause que se detengan sus operaciones o se pierdan datos. Las políticas de recuperación ante desastres dictan la forma en que la organización restaura sus operaciones e información para volver a la misma capacidad operativa que antes del evento. La continuidad del negocio es el plan al que recurre la organización cuando intenta operar sin determinados recursos.
- La capacitación del usuario final aborda el factor de ciberseguridad más impredecible: las personas. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro. Enseñarles a los usuarios a eliminar los archivos adjuntos de correos electrónicos sospechosos, a no conectar unidades USB no identificadas y otras lecciones importantes es fundamental para la seguridad de cualquier organización.



La extensión de las ciberamenazas

Las ciberamenazas mundiales siguen desarrollándose a un ritmo rápido, con una cantidad cada vez mayor de filtraciones de datos cada año. En un informe de RiskBased Security, se reveló que unos alarmantes 7900 millones de registros han sido expuestos por filtraciones de datos solo en los primeros nueve meses del 2019. Esta cifra es más del doble (112 %) de la cantidad de registros expuestos en el mismo período durante el 2018.

Los servicios médicos, los minoristas y las entidades públicas fueron los que sufrieron más filtraciones, y los delincuentes maliciosos fueron los responsables de la mayoría de los incidentes. Algunos de estos sectores son más atractivos para los cibercriminales, ya que recopilan datos financieros y médicos, aunque todas las empresas que utilizan las redes pueden ser atacadas para robarles datos de clientes, hacer espionaje corporativo o lanzar ataques a sus clientes.

Tipos de ciberamenazas:

Las amenazas a las que se enfrenta la ciberseguridad son tres:

- El delito cibernético incluye agentes individuales o grupos que atacan a los sistemas para obtener beneficios financieros o causar interrupciones.
- Los ciberataques a menudo involucran la recopilación de información con fines políticos.
- El ciberterrorismo tiene como objetivo debilitar los sistemas electrónicos para causar pánico o temor.



-Pero ¿cómo consiguen los agentes malintencionados el control de los sistemas informáticos? Estos son algunos de los métodos comunes utilizados para amenazar la ciberseguridad:

Malware:

“Malware” se refiere al software malicioso. Ya que es una de las ciberamenazas más comunes, el malware es software que un cibercriminal o un hacker ha creado para interrumpir o dañar el equipo de un usuario legítimo. Con frecuencia propagado a través de un archivo adjunto de correo electrónico no solicitado o de una descarga de apariencia legítima, el malware puede ser utilizado por los ciberdelincuentes para ganar dinero o para realizar ciberataques con fines políticos.

Hay diferentes tipos de malware, entre los que se incluyen los siguientes:

- **Virus:** un programa capaz de reproducirse, que se incrusta un archivo limpio y se extiende por todo el sistema informático e infecta a los archivos con código malicioso.
- **Troyanos:** un tipo de malware que se disfraza como software legítimo. Los cibercriminales engañan a los usuarios para que carguen troyanos a sus computadoras, donde causan daños o recopilan datos.
- **Spyware:** un programa que registra en secreto lo que hace un usuario para que los cibercriminales puedan hacer uso de esta información. Por ejemplo, el spyware podría capturar los detalles de las tarjetas de crédito.
- **Ransomware:** malware que bloquea los archivos y datos de un usuario, con la amenaza de borrarlos, a menos que se pague un rescate.
- **Adware:** software de publicidad que puede utilizarse para difundir malware.
- **Botnets:** redes de computadoras con infección de malware que los cibercriminales utilizan para realizar tareas en línea sin el permiso del usuario.



Inyección de código SQL

Una inyección de código SQL (por sus siglas en inglés Structured Query Language) es un tipo de ciberataque utilizado para tomar el control y robar datos de una base de datos. Los cibercriminales aprovechan las vulnerabilidades de las aplicaciones basadas en datos para insertar código malicioso en una base de datos mediante una instrucción SQL maliciosa. Esto les brinda acceso a la información confidencial contenida en la base de datos.

Phishing

El phishing es cuando los cibercriminales atacan a sus víctimas con correos electrónicos que parecen ser de una empresa legítima que solicita información confidencial. Los ataques de phishing se utilizan a menudo para inducir a que las personas entreguen sus datos de tarjetas de crédito y otra información personal.

Ataque de tipo “Man-in-the-middle”

Un ataque de tipo “Man-in-the-middle” es un tipo de ciberamenaza en la que un cibercriminal intercepta la comunicación entre dos individuos para robar datos. Por ejemplo, en una red Wi-Fi no segura, un atacante podría interceptar los datos que se transmiten desde el dispositivo de la víctima y la red.

Ataque de denegación de servicio

Un ataque de denegación de servicio es cuando los cibercriminales impiden que un sistema informático satisfaga solicitudes legítimas sobrecargando las redes y los servidores con tráfico. Esto hace que el sistema sea inutilizable e impide que una organización realice funciones vitales.



Ciberamenazas más recientes

¿Cuáles son las ciberamenazas más recientes contra las que deben protegerse las personas y las organizaciones? A continuación, se presentan algunas de las ciberamenazas más recientes comunicadas por los gobiernos de Estados Unidos, Australia y el Reino Unido.


- En diciembre del 2019, el Departamento de Justicia de los Estados Unidos (DoJ) imputó al líder de un grupo de cibercriminales organizados por su participación en un ataque global del malware Dridex. Esta campaña malintencionada afectó al público, al gobierno, a la infraestructura y a las empresas de todo el mundo. Dridex es un troyano financiero que posee diferentes funcionalidades. Desde el 2014, afecta a las víctimas e infecta a las computadoras a través de correos electrónicos de phishing o malware existente. Es capaz de robar contraseñas, datos bancarios y datos personales que pueden utilizarse en transacciones fraudulentas, y ha causado pérdidas financieras masivas que suman cientos de millones de dólares. En respuesta a los ataques de Dridex, el Centro Nacional de Seguridad Cibernética del Reino Unido aconseja a las personas que “se aseguren de que los dispositivos estén actualizados y los antivirus estén activados y actualizados, y de que se realicen copias de seguridad de los archivos”.
- Estafas románticas: En febrero del 2020, el FBI advirtió a los ciudadanos de EE. UU. que tuvieran cuidado con el fraude a la confianza que los cibercriminales cometen a través de sitios de citas, salas de chat y aplicaciones. Los perpetradores se aprovechan de las personas que buscan nuevas parejas y engañan a las víctimas para que proporcionen sus datos personales. El FBI informa que las ciberamenazas románticas afectaron a 114 víctimas de Nuevo México durante 2019, cuyas pérdidas financieras sumaron 1 600 000 dólares.
- Malware Emotet: A finales del 2019, el Centro Australiano de Seguridad Cibernética advirtió a las organizaciones nacionales sobre la ciberamenaza mundial generalizada del malware Emotet. Emotet es un sofisticado troyano que puede robar datos y también cargar otros malware. Emotet se aprovecha de las contraseñas poco sofisticadas y es un recordatorio de la importancia de crear una contraseña segura para protegerse de las ciberamenazas.



consejos de ciberseguridad:

- Actualizar el software y el sistema operativo: esto significa que aprovechará las últimas revisiones de seguridad.
- Utilizar software antivirus: las soluciones de seguridad, como Kaspersky Total Security, detectarán y eliminarán las amenazas. Mantenga su software actualizado para obtener el mejor nivel de protección.
- Utilizar contraseñas seguras: asegúrese de que sus contraseñas no sean fáciles de adivinar.
- No abrir archivos adjuntos de correos electrónicos de remitentes desconocidos: podrían estar infectados con malware.
- No hacer clic en los vínculos de los correos electrónicos de remitentes o sitios web desconocidos: es una forma común de propagación de malware.
- Evitar el uso de redes Wi-Fi no seguras en lugares públicos: las redes no seguras lo dejan vulnerable a ataques del tipo “Man-in-the-middle”.



Instrumento de Evaluación de las Evidencias			
Indicadores o criterios de desempeño/competencias del aprendizaje esperado			
Evidencias	Aún no logrado	En Proceso	Logrado
 Distinguir las características del ámbito de la ciberseguridad, sus principios y las medidas de seguridad cibernética.			

Rúbrica

Criterio	Puntaje	Descripción
Aún no logrado	1	El estudiante desconoce los conceptos, procedimientos, operaciones necesarias para obtener la evidencia solicitada.
En proceso	2	El estudiante conoce algunos de los conceptos, procedimientos, operaciones necesarias para obtener la evidencia solicitada, pero no llega a obtenerla del todo.
Logrado	3	El estudiante demuestra que logra obtener la evidencia solicitada.