:

UNIDAD I. INVESTIGACIÓN 20%

RÚBRICA PARA EVALUAR UN TRABAJO DE INVESTIGACIÓN (20 puntos)

ALUMNO: Román Omar Fiscal Polito

Criterio	Excelente (5)	Bueno (4)	Aceptable (3)	Insuficiente (1-2)	Puntos
Revisión de literatura	Actual, relevante y bien citada	Pertinente, aunque algo limitada	Escasa o poco relevante	Ausente o plagio	5
Metodología	Clara, adecuada y coherente con objetivos	Adec. aunque con mínimos errores o ambig.	Ambigua o poco detallada	Inapropiada o ausente	5
Resultados y análisis	Presentados con claridad y análisis crítico	Presentados con buena estructura	Parcialmente analizados	Incompletos o mal presentados	5
Presentación escrita	Redacción impecable, buena estructura y citas	Buena presentación, con pocos errores	Presentación aceptable, errores frecuentes	Desordenada, difícil de seguir	5

Total: /20

INSTITUTO TECNOLÓGICO SUPERIOR DE SAN ANDRÉS TUXTLA

Seguridad Informática

Investigación - Unidad I

M.T.I Juan Rafael González Cadena

Román Omar Fiscal Polito

GRUPO: 810 **UNIDAD: 1**

Seguridad informática: ¿en qué consiste?

Se conoce como seguridad informática al proceso de prevenir y detectar amenazas en los sistemas informáticos que puedan poner en riesgo, sobre todo, la data. Esta rama de la ciberseguridad se encarga de mantener lejos de las manos de intrusos todos los recursos informáticos y de data, que suelen ser vulnerados con el objetivo de cometer fraude, hacer extorsiones o vender la información.

La seguridad informática se compone de una serie específica de procesos que abarcan desde software antivirus, firewalls y otras medidas especializadas acorde al sistema informático en cuestión, qué recursos de red tenemos y otras particularidades. La idea es que mediante un plan de acción puedas abarcar problemas de confidencialidad, autorizaciones, disponibilidad y autenticación sin correr el riesgo de que tus datos sean modificados, borrados o robados por una brecha de seguridad.

La seguridad informática es muy importante para cualquier sector empresarial, pero el área de las finanzas y hospitales la ha encontrado de vital importancia. El sector bancario tiene que contar con la seguridad informática más efectiva para mantener a salvo la información de cuentas, tarjetas, contraseñas y registros, mientras que los hospitales deben mantener un registro riguroso de los pacientes, diagnósticos y pagos. Ambos sectores podrían entrar en una crisis si ocurriera un percance con su seguridad y con el robo de datos de su área.

Sin embargo, el resto de los sectores comerciales no está exento de ataques y tampoco importa si se trata de una empresa pequeña o grande, los datos se han convertido en un bien inmaterial pero muy valioso, y es importante mantenerlos siempre seguros.

Así es como los expertos en seguridad informática se han vuelto imprescindibles para el sector empresarial. Todos aquellos preparados para crear protocolos de seguridad han encontrado muchas entradas laborales en terrenos delicados que requieren mucha preparación. Cada compañía tiene sus propios jefes de seguridad y también sus propias necesidades en cuanto a certificaciones y entrenamiento. Por suerte, CompuEducación cuenta con una amplia gama de cursos de

Ciberseguridad orientadas a distintas áreas, desde el análisis y la implementación hasta la recuperación y el control de daños, ¡contáctanos!

En los últimos años, la seguridad informática se ha convertido en un tema de interés público. Tanto expertos en la materia como usuarios generales utilizan términos como "clave de usuario", "contraseña (o password)", "fraude informático", "hacker", etcétera. Hoy por hoy no solo es deseable, sino indispensable, tener conocimientos firmes relacionados con este tema, pues sin ellos el usuario de computadoras podría caer en un estado de indefensión que ponga en peligro no solo su informaciónn o equipo, sino su propia integridad.

Gómez (2006) define la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, equipo o software. Por su parte, Kissel (2012) la define como la protección de información y sistemas de información de acceso no autorizado. En efecto, con base en estos conceptos, la seguridad informática se vincula con tres elementos básicos: la informaci6n que, como activo intangible, representa quizá el elemento más sensible y vulnerable; el software, cuya pérdida o modificación mal intencionada puede representar severos quebrantos económicos u operativos no solo hacia el usuario sino a toda una institución; y el hardware, que al fallar provoca retrasos en la operación diaria y la consecuente pérdida de tiempo y costos elevados.

Existe un sin número de medidas preventivas que permiten proteger estos tres elementos, como respaldos de informaci6n (backups), controles de acceso de hardware y software, programas antivirus, antispyware y antispam, uso de firewalls, actualizaciones continuas al sistema operativo, mantenimiento al equipo de c6mputo y protección física en las áreas de operaciones de red (extintores, detectores de humo y calor, sistemas de anclaje, ventilaci6n, controles de temperatura y humedad, reguladores de voltaje, sistemas de suministro continuo de energía, entre otros).

Sin embargo, para un usuario, la protección de su información es generalmente más importante que la protección misma del software o su equipo, razón por la cual, para garantizar la seguridad de los datos, es precise cumplir con tres componentes

fundamentales: integridad, que significa que la información debe ser modificada solo por entidades autorizadas; disponibilidad, es decir, tener acceso a la información cuando se lo requiera; y confidencialidad, donde solo instancias facultadas para ello podrán visualizar los datos.

Debido a la importancia que ha ido adquiriendo la seguridad en cómputo, en las siguientes ediciones de cápsulas TI se abordarán en detalle recomendaciones diversas que permitan evitar posibles pérdidas de datos, robos de información, accesos no autorizados, suplantación de identidad, presencia de malware, entre otros.

Rúbrica de Evaluación de Exposición Oral

Fiscal Polito Román Omar

Esta rúbrica permite evaluar presentaciones orales con un puntaje máximo de 40 puntos. Está organizada en 5 criterios, cada uno con un valor máximo de 10 puntos.

Criterio	Excelente (10 pts)	Bueno (8 pts)	Regular (5 pts)	Insuficiente (1-2 pts)
Contenido y dominio del tema	Expone con profundidad, demuestra dominio y aporta ideas claras y bien estructuradas.	Muestra buen conocimiento, aunque con algunas omisiones menores.	Conoce el tema de forma superficial, hay falta de claridad en algunos puntos.	Demuestra poco conocimiento, se observan errores conceptuales.
Organización y estructura	La exposición sigue un orden lógico con introducción, desarrollo y cierre claro.	El orden es adecuado, aunque con ligeras interrupciones en la secuencia.	Organización poco clara, se pierde el hilo en algunos momentos.	Desorganizada, sin coherencia ni estructura evidente.
Claridad y lenguaje técnico	Utiliza lenguaje apropiado, técnico y comprensible para la audiencia.	Usa lenguaje adecuado con algunas imprecisiones técnicas.	Emplea términos vagos o poco precisos, algunas expresiones confusas.	Uso incorrecto del lenguaje, jerga o tecnicismos mal aplicados.
Recursos y apoyos visuales	Apoya la exposición con recursos bien diseñados y relevantes (diapositivas, videos).	Usa apoyos visuales adecuados, aunque podrían estar mejor integrados.	Recursos poco útiles o mal empleados, no aportan al mensaje.	No utiliza recursos, o los usados distraen o restan claridad.
Comunicación y lenguaje no verbal	Muestra seguridad, contacto visual, buena entonación y lenguaje corporal adecuado.	Buena comunicación, aunque con momentos de inseguridad o poca expresión.	Dificultad para mantener la atención, tono monótono o gestos limitados.	No se comunica con claridad, lectura excesiva, falta de contacto visual.

Calificación 35%

Principales Amenazas en Internet Internet 2025

Las amenazas cibernéticas evolucionan rápidamente, afectando a empresas, usuarios y empresas, usuarios y servicios críticos. Este informe detalla los riesgos emergentes y emergentes y cómo protegerse en 2025. Se anticipa un crecimiento significativo en significativo en ataques de phishing y vulnerabilidades en dispositivos IoT, con un con un impacto global cada vez mayor.

Ransomware: La Amenaza Más Sofisticada

Ataques Dirigidos

El ransomware apunta a sectores críticos como hospitales y sistemas sistemas financieros.

Doble Extorsión

Ahora combinan cifrado de datos con con amenazas de filtración pública. pública.

Impacto Creciente

Los rescates son cada vez más altos, altos, causando daño reputacional y reputacional y financiero.

Phishing Avanzado Impulsado por IA

Personalización con IA

La inteligencia artificial genera mensajes de phishing altamente altamente personalizados.

Aumento de Ataques

Se registra un incremento del 35% en ataques de phishing en 2024. 2024.

Múltiples Canales

Los ataques se extienden a email, SMS (smishing) y llamadas (vishing). (vishing).

Vulnerabilidades en Dispositivos IoT

Dispositivos IoT

75B

Dispositivos IoT

Se estiman 75 mil millones de dispositivos IoT para 2025.

60%

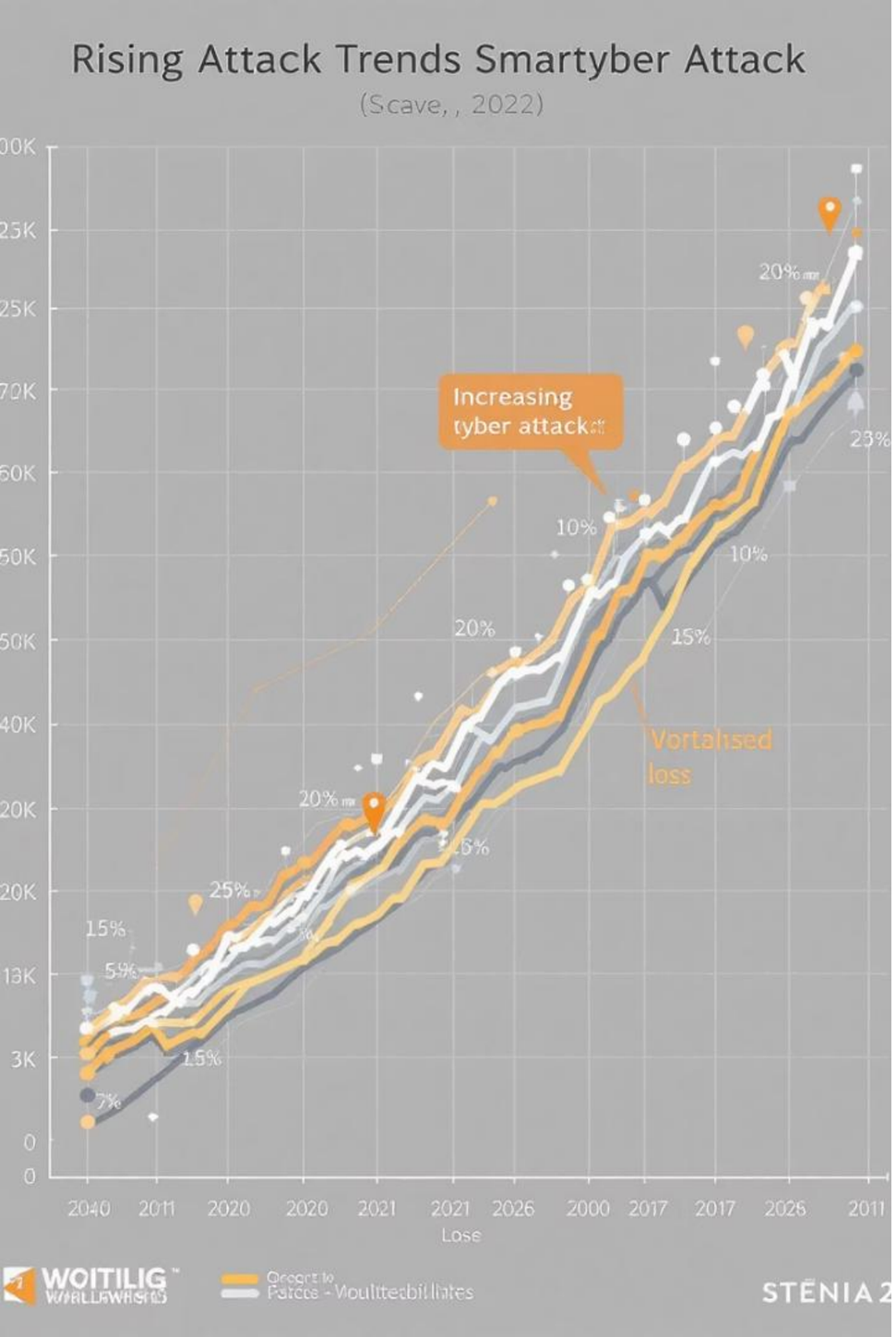
Dispositivos Críticos Críticos

60% de dispositivos empresariales IoT presentan vulnerabilidades críticas. críticas.

3

Riesgos

Ciudades inteligentes, industria y hogares conectados están en riesgo.



Estadísticas y Tendencias Alarmantes

Ransomware	Paralizó sistema de salud en Irlanda Irlanda (2021).
Costo Estimado	$265 mil millones en pérdidas globales para 2031.
IoT	60% de dispositivos corporativos con con vulnerabilidades.

Ejemplos de Impacto Real

Salud y Finanzas

Hospitales y bancos han sido paralizados por ataques de ransomware.

Empresas

Víctimas de phishing sufren robo de datos y fraudes financieros.

IoT Industrial

Cámaras y sensores industriales son "puertas de entrada" para hackers.

Nuevas Técnicas y Evolución de de Amenazas

IA Criminal

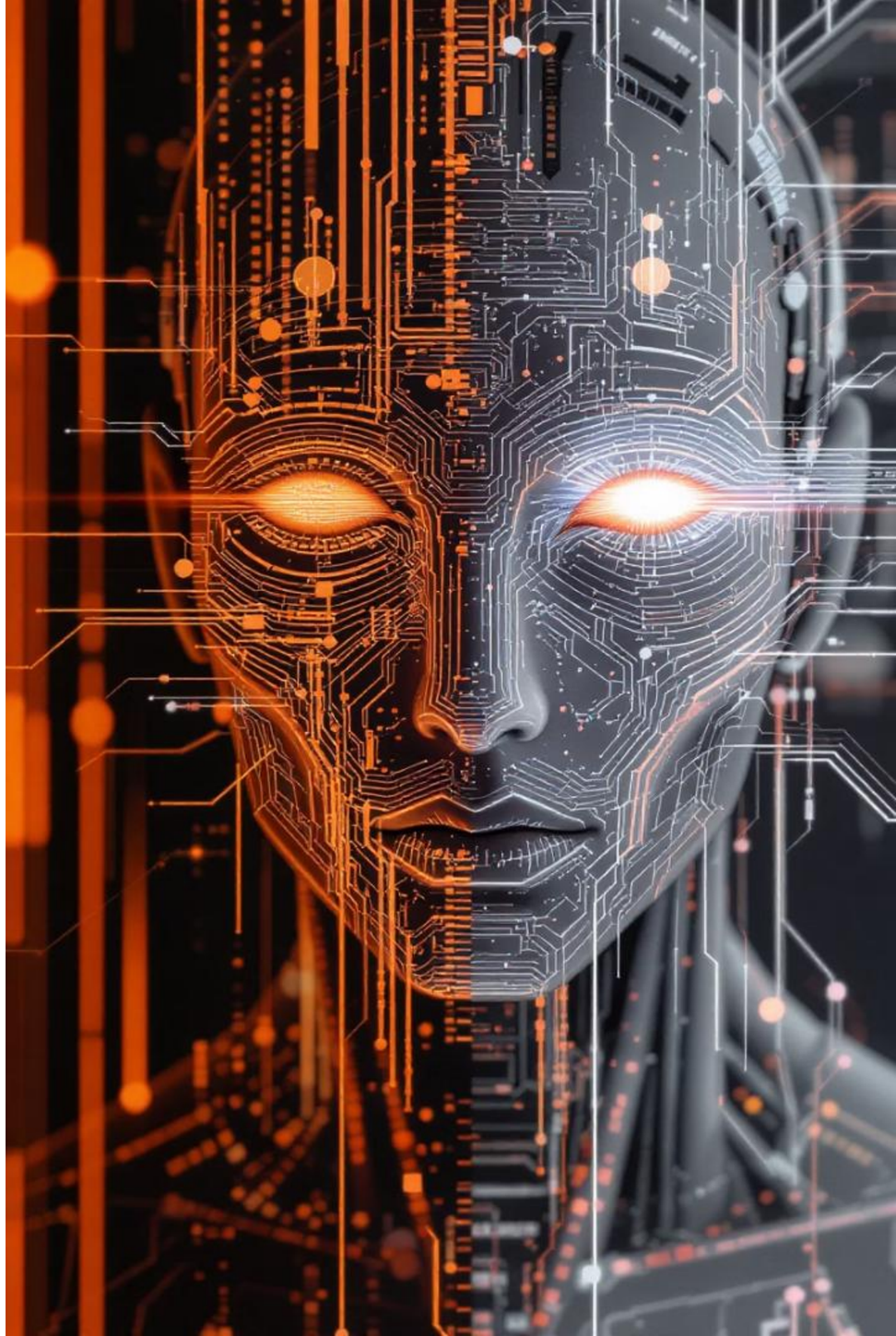
Automatización con IA y deepfakes para ataques.

Ingeniería Social

Técnicas sofisticadas y ataques a la cadena de suministros.

Mensajería

Explotación de plataformas de mensajería y redes sociales.



Cómo Protegerse Hoy

Copias y Actualizaciones

Realice copias de seguridad y actualizaciones de software con frecuencia. frecuencia.

Seguridad Avanzada

Implemente soluciones de seguridad contra comportamientos anómalos. anómalos.

Capacitación

Eduque al personal sobre amenazas y reconocimiento de fraudes.

IoT Seguro

Revise constantemente las configuraciones de seguridad en dispositivos IoT. dispositivos IoT.

EXAMEN 40%

Román Omar Fiscal Polita **CALIF: 40**

1. El conjunto de medidas destinadas a paliar los daños en un equipo informático una vez que ha recibido un ataque reciben el nombre de

A) seguridad pasiva
B) seguridad activa
C) seguridad lógica

2. Los virus que se introducen en el equipo camuflados dentro de otros programas reciben el nombre de

A) keyloggers
B) troyanos
C) gusanos

3. El envío de correos electrónicos fraudulentos para conseguir los datos bancarios de personas recibe el nombre de

A) cracking
B) pharming
C) phising

4. El programa que controla el tráfico de información a través de los puertos de entrada de un ordenador se llama

A) antispam
B) antivirus
C) cortafuegos

5. El software de código abierto, cuyo código de programación se puede conocer y modificar, recibe el nombre de

A) software libre
B) software freeware
C) software comercial

6. El análisis de los datos de navegación de la gente para sacar conclusiones sobre, por ejemplo, sus hábitos de compra, forma parte de

A) internet de las cosas
B) plan de seguridad informática
C) big data

7. ¿Qué son las cookies?

A) archivos de publicidad que nos anuncian productos
B) archivos de texto que guarda el navegador con datos recogidos en las webs que

hemos visitado
C) virus que navegan por internet

8. Un protocolo de transmisión de datos cifrado
A) sirve únicamente para la comunicación de datos bancarios
B) es un sistema de intercambio de correos electrónicos seguro
C) encripta la información que se comparte por internet

9. Un sistema de restauración de un equipo informático

A) realiza una copia de seguridad diaria de sus archivos
B) recupera la integridad de su placa base si ha sido dañada
C) cambia el software de un ordenador para dejarlo como era antes de sufrir cambios no deseados

10. Para identificarnos ante la administración pública en internet necesitamos

A) una contraseña segura
B) siempre el dni electrónico
C) un certificado electrónico adecuado