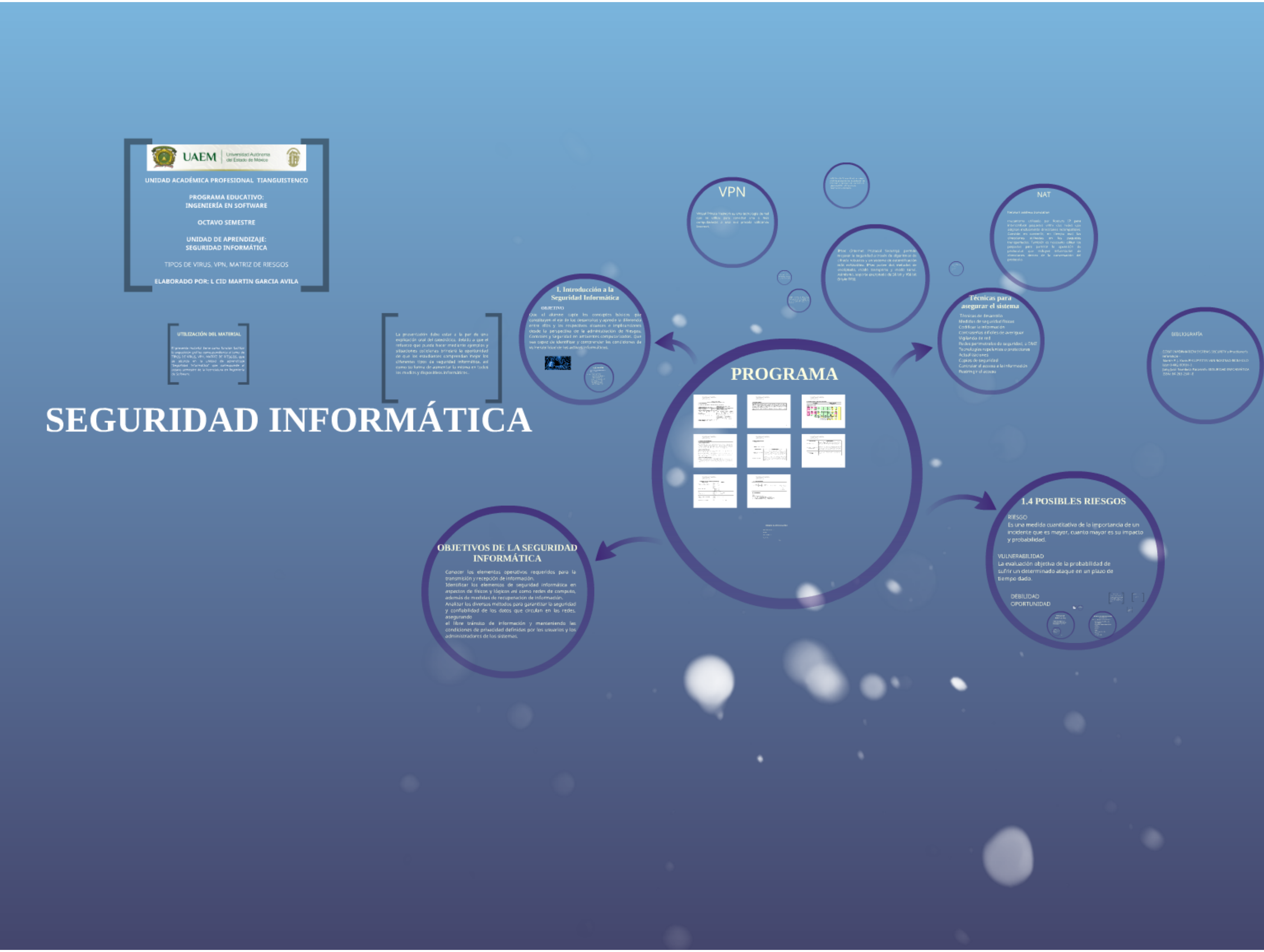

UAEM Universidad Autónoma del Estado de México
UNIDAD ACADÉMICA PROFESIONAL TIANGUISTENCO
PROGRAMA EDUCATIVO:
INGENIERÍA EN SOFTWARE
OCTAVO SEMESTRE
UNIDAD DE APRENDIZAJE:
SEGURIDAD INFORMÁTICA
TIPOS DE VIRUS, VPN, MATRIZ DE RIESGOS
ELABORADO POR: L CID MARTIN GARCIA AVILA
UTILIZACIÓN DEL MATERIAL
La presentación debe estar a la par de una explicación oral del catedrático, debido a que el refuerzo que pueda hacer mediante ejemplos y situaciones cotidianas brindará la oportunidad de que los estudiantes comprendan mejor los diferentes tipos de seguridad informática, así como su forma de aumentar la misma en todos los medios y dispositivos informáticos.
SEGURIDAD INFORMÁTICA
I. Introducción a la Seguridad Informática
OBJETIVO
Que el alumno capte los conceptos básicos que constituyen el eje de los desarrollos y aprecie la diferencia entre ellos y los respectivos alcances e implicaciones desde la perspectiva de la administración de Riesgos, Controles y Seguridad en ambientes computarizados. Que sea capaz de identificar y comprender las condiciones de vulnerabilidad de los activos informáticos.
VPN
NAT
PROGRAMA
Técnicas para asegurar el sistema
Técnicas de desarrollo
Medidas de seguridad físicas
Codificar la información
Contraseñas difíciles de averiguar
Vigilancia de red
Redes perimetrales de seguridad, o DMZ
Tecnologías repelentes o protectoras
Actualizaciones
Copias de seguridad
Controlar el acceso a la información
Restringir el acceso
BIBLIOGRAFÍA
OBJETIVOS DE LA SEGURIDAD INFORMÁTICA
Conocer los elementos operativos requeridos para la transmisión y recepción de información.
Identificar los elementos de seguridad informática en aspectos de físicos y lógicos así como redes de computo, además de medidas de recuperación de información.
Analizar los diversos métodos para garantizar la seguridad y confiabilidad de los datos que circulan en las redes, asegurando
el libre tránsito de información y manteniendo las condiciones de privacidad definidas por los usuarios y los administradores de los sistemas.
1.4 POSIBLES RIESGOS
RIESGO
Es una medida cuantitativa de la importancia de un incidente que es mayor, cuanto mayor es su impacto y probabilidad.
VULNERABILIDAD
La evaluación objetiva de la probabilidad de sufrir un determinado ataque en un plazo de tiempo dado.
DEBILIDAD
OPORTUNIDAD

UAEM | Universidad Autónoma del Estado de México

UNIDAD ACADÉMICA PROFESIONAL TIANGUISTENCO

PROGRAMA EDUCATIVO:
INGENIERÍA EN SOFTWARE

OCTAVO SEMESTRE

UNIDAD DE APRENDIZAJE:
SEGURIDAD INFORMÁTICA

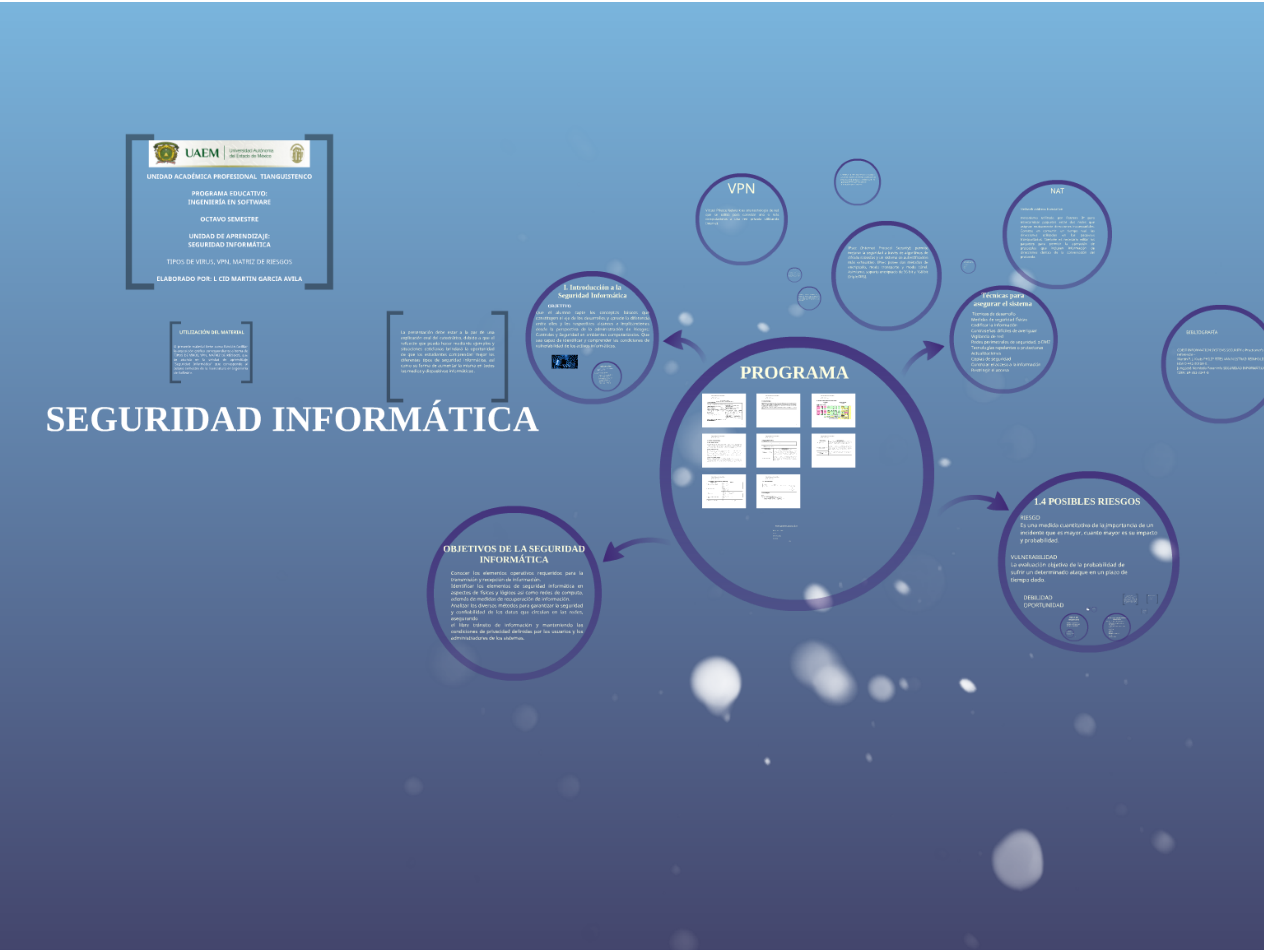
TIPOS DE VIRUS, VPN, MATRIZ DE RIESGOS

ELABORADO POR: L CID MARTIN GARCIA AVILA

UTILIZACIÓN DEL MATERIAL

El presente material tiene como función facilitar la exposición gráfica correspondiente al tema de TIPOS DE VIRUS, VPN, MATRIZ DE RIESGOS, que se aborda en la unidad de aprendizaje “Seguridad Informática" que corresponde al octavo semestre de la licenciatura en Ingeniería de Software.

La presentación debe estar a la par de una explicación oral del catedrático, debido a que el refuerzo que pueda hacer mediante ejemplos y situaciones cotidianas brindará la oportunidad de que los estudiantes comprendan mejor los diferentes tipos de seguridad informática, así como su forma de aumentar la misma en todos los medios y dispositivos informáticos .


UAEM Universidad Autónoma del Estado de México
UNIDAD ACADÉMICA PROFESIONAL TIANGUISTENCO
PROGRAMA EDUCATIVO:
INGENIERÍA EN SOFTWARE
OCTAVO SEMESTRE
UNIDAD DE APRENDIZAJE:
SEGURIDAD INFORMÁTICA
TIPOS DE VIRUS, VPN, MATRIZ DE RIESGOS
ELABORADO POR: L CID MARTIN GARCIA AVILA
UTILIZACIÓN DEL MATERIAL
La presentación debe estar a la par de una explicación oral del catedrático, debido a que el refuerzo que pueda hacer mediante ejemplos y situaciones cotidianas brindará la oportunidad de que los estudiantes comprendan mejor los diferentes tipos de seguridad informática, así como su forma de aumentar la misma en todos los medios y dispositivos informáticos.
SEGURIDAD INFORMÁTICA
1. Introducción a la Seguridad Informática
OBJETIVO
Que el alumno capte los conceptos básicos que constituyen el eje de los desarrollos y aprecie la diferencia entre ellos y los respectivos alcances e implicaciones desde la perspectiva de la administración de Riesgos; Controles y Seguridad en ambientes computarizados. Que sea capaz de identificar y comprender las condiciones de vulnerabilidad de los activos informáticos.
VPN
Virtual Private Network es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.
IPsec (Internet Protocol Security) permite mejorar la seguridad a través de algoritmos de cifrado robustos y un sistema de autentificación más exhaustivo. IPsec posee dos métodos de encriptado, modo transporte y modo túnel. Asimismo, soporta encriptado de 56 bit y 168 bit (Triple DES).
NAT
Network Address Translation
Técnicas para asegurar el sistema
Técnicas de desarrollo
Medidas de seguridad físicas
Codificar la información
Contraseñas difíciles de averiguar
Vigilancia de red
Redes perimetrales de seguridad, o DMZ
Tecnologías repelentes o protectoras
Actualizaciones
Copias de seguridad
Controlar el acceso a la información
Restringir el acceso
PROGRAMA
BIBLIOGRAFÍA
1.4 POSIBLES RIESGOS
RIESGO
Es una medida cuantitativa de la importancia de un incidente que es mayor, cuanto mayor es su impacto y probabilidad.
VULNERABILIDAD
La evaluación objetiva de la probabilidad de sufrir un determinado ataque en un plazo de tiempo dado.
DEBILIDAD
OPORTUNIDAD
OBJETIVOS DE LA SEGURIDAD INFORMÁTICA
Conocer los elementos operativos requeridos para la transmisión y recepción de información.
Identificar los elementos de seguridad informática en aspectos de físicos y lógicos así como redes de computo, además de medidas de recuperación de información.
Analizar los diversos métodos para garantizar la seguridad y confiabilidad de los datos que circulan en las redes, asegurando
el libre tránsito de información y manteniendo las condiciones de privacidad definidas por los usuarios y los administradores de los sistemas.

I. Introducción a la Seguridad Informática

OBJETIVO

Que el alumno capte los conceptos básicos que constituyen el eje de los desarrollos y aprecie la diferencia entre ellos y los respectivos alcances e implicanciones desde la perspectiva de la administración de Riesgos; Controles y Seguridad en ambientes computarizados. Que sea capaz de identificar y comprender las condiciones de vulnerabilidad de los activos informáticos.

Información

Conjunto de datos organizados que tienen un significado. (Soporte)

TIPOS DE INFORMACIÓN

- Información privilegiada
- Información pública
- Información confidencial
- Información externa
- Información interna
- Información personal


www@

Información

Conjunto de datos organizados que tienen un significado. (Soporte)

TIPOS DE INFORMACIÓN

- Información privilegiada
- Información pública
- Información confidencial
- Información externa
- Información interna
- Información personal

OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

Conocer los elementos operativos requeridos para la transmisión y recepción de información.

Identificar los elementos de seguridad informática en aspectos de físicos y lógicos asi como redes de computo, además de medidas de recuperación de información.

Analizar los diversos métodos para garantizar la seguridad y confiabilidad de los datos que circulan en las redes, asegurando

el libre tránsito de información y manteniendo las condiciones de privacidad definidas por los usuarios y los administradores de los sistemas.

1.4 POSIBLES RIESGOS

RIESGO
Es una medida cuantitativa de la importancia de un incidente que es mayor, cuanto mayor es su impacto y probabilidad.

VULNERABILIDAD
La evaluación objetiva de la probabilidad de sufrir un determinado ataque en un plazo de tiempo dado.

DEBILIDAD
OPORTUNIDAD

TIPOS DE AMENAZAS

AMENAZAS TERCIARIAS
AMENAZAS SECUNDARIAS
AMENAZAS PRIMARIAS

LAS AMENAZAS

- El usuario: causa del mayor problema
- Programas maliciosos: virus.
- Un intruso: (cracker, defacer, script kiddie o Script boy, viruxer, etc.).
- Un siniestro (robo, incendio, inundación): una mala manipulación o una malintención derivan a la pérdida del material o de los archivos.
- El personal interno de Sistemas.

LAS AMENAZAS

- El usuario: causa del mayor problema
- Programas maliciosos: virus.
- Un intruso: (cracker, defacer, script kiddie o Script boy, viruxer, etc.).
- Un siniestro (robo, incendio, inundación): una mala manipulación o una malintención derivan a la pérdida del material o de los archivos.
- El personal interno de Sistemas.

Tipos de Virus

Virus residentes
La característica principal de estos virus es que se ocultan en la memoria RAM de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros.

Virus de acción directa
Al contrario que los residentes, estos virus no permanecen en memoria. Por tanto, su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos.

Virus de sobre escritura
Estos virus se caracterizan por destruir la información contenida en los ficheros que infectan. Cuando infectan un fichero, escriben dentro de su contenido, haciendo que queden total o parcialmente inservibles.

Tipos de Virus

Virus cifrados
Más que un tipo de virus, se trata de una técnica utilizada por algunos de ellos, que a su vez pueden pertenecer a otras clasificaciones. Estos virus se cifran a sí mismos para no ser detectados por los programas antivirus.

Virus del Fichero
Infectan programas o ficheros ejecutables (ficheros con extensiones EXE y COM). Al ejecutarse el programa infectado, el virus se activa, produciendo diferentes efectos.

Virus de enlace o directorio
Los ficheros se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos.

Tipos de Virus

Virus multipartites
Virus muy avanzados, que pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc.

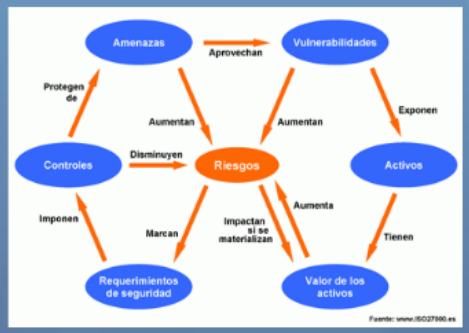
Virus de FAT
Es la sección de un disco utilizada para enlazar la información contenida en éste. Se trata de un elemento fundamental en el sistema. Los virus que atacan a este elemento son especialmente peligrosos, ya que impedirán el acceso a ciertas partes del disco.

Virus polimórficos
Son virus que en cada infección que realizan se cifran de una forma distinta. De esta forma, generan una elevada cantidad de copias de sí mismos e impiden que los antivirus los localicen a través de la búsqueda de cadenas o firmas, por lo que suelen ser los virus más costosos de detectar.

RIESGO

Es todo tipo de vulnerabilidades, amenazas que pueden ocurrir sin previo aviso y producir numerosas pérdidas para las empresas.

MATRIZ DE RIESGOS



* * * * * * Matriz De Riesgo * * * * * *

Riesgo	Probabilidad	Impacto
Caida de la red	Media	Alto
Caida de servicios de producción	Media	Bajo
Extracción, modificación y destrucción de información confidencial	Baja	Alto
Uso inadecuado de las instalaciones	Alta	Media
Ataques de virus informáticos	Alta	Alto
Fuga de información	Media	Alto
Inadecuados controles de acceso lógicos	Baja	Alto
Pérdida de información	Baja	Media
Falta de disponibilidad de aplicaciones críticas	Baja	Alto
Descontrol del personal	Media	Baja


Amenazas
Aprovechan
Vulnerabilidades
Protegen de
Aumentan
Aumentan
Exponen
Controles
Disminuyen
Riesgos
Activos
Imponen
Marcan
Impactan si se materializan
Aumenta
Tienen
Requerimientos de seguridad
Valor de los activos
Fuente: www.ISO27000.es

Matriz de Análisis de Riesgo		**Probabilidad de Amenaza**					
Elementos de Información	**Magnitud de Daño**	Criminalidad		Sucesos físicos		Negligencia	
		Robo	Virus	Incendio	Falta de Corriente	Compartir contraseñas	No cifrar datos criticos
Datos e Información							
RR.HH							
Finanzas							
Sistema e Información							
Computadoras							
Portátiles							
Personal							
Coordinador							
Personal técnico							

de seguridad

activos

Fuente: www.ISO27000.es

****** Matriz De Riesgo ******

Riesgo	Probabilidad	Impacto
Caida de la red	Media	Alto
Caida de servicios de producción	Media	Bajo
Extracción, modificación y destrucción de información confidencial	Baja	Alto
Uso inadecuado de las instalaciones	Alta	Media
Ataques de virus informáticos	Alta	Alto
Fuga de información	Media	Alto
Inadecuados controles de acceso lógicos	Baja	Alto
Pérdida de información	Baja	Media
Falta de disponibilidad de aplicaciones críticas	Baja	Alto
Descontrol del personal	Media	Baja

TÉCNICAS DE ASEGURAMIENTO DEL SISTEMA

TÉCNICAS QUE MITIGAN AMENAZAS TERCIARIAS

- Eliminación de oportunidades
- Redundancia
- Control de accesos lógico y físico
- Cifrado
- Camuflaje
- Reserva
- Seguros
- Inventario y Marcado
- Blindaje
- No hacer nada

Aspectos que debe cubrir la seguridad informática

- Confidencialidad
- Confiabilidad

CONFIDENCIALIDAD

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas.

- Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla.
- Cuando se publica información privada.
- Cuando un laptop con información sensible sobre una empresa es robado.
- Cuando se divulga información confidencial a través del teléfono, etc.

Todos estos casos pueden constituir una violación de la confidencialidad.

Técnicas para asegurar el sistema

Técnicas de desarrollo
Medidas de seguridad físicas
Codificar la información
Contraseñas difíciles de averiguar
Vigilancia de red
Redes perimetrales de seguridad, o DMZ
Tecnologías repelentes o protectoras
Actualizaciones
Copias de seguridad
Controlar el acceso a la información
Restringir el acceso

VPN

Virtual Private Network es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

IPsec (Internet Protocol Security): permite mejorar la seguridad a través de algoritmos de cifrado robustos y un sistema de autentificación más exhaustivo. IPsec posee dos métodos de encriptado, modo transporte y modo túnel. Asimismo, soporta encriptado de 56 bit y 168 bit (triple DES).

lada por un
mpresas. PPTP
ifrado de 40 bit
crosoft Point to
i solo no cifra la

L2TP/IPsec (L2TP sobre IPsec): tecnología capaz de proveer el nivel de protección de IPsec sobre el protocolo de túnel L2TP. Al igual que PPTP, L2TP no cifra la información por sí mismo.

PPTP/MPPE: tecnología desarrollada por un consorcio formado por varias empresas. PPTP soporta varios protocolos VPN con cifrado de 40 bit y 128 bit utilizando el protocolo Microsoft Point to Point Encryption (MPPE). PPTP por sí solo no cifra la información.

Implementaciones

El protocolo estándar de facto es el IPSEC, pero también están PPTP, L2F, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.

Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software. Dentro de esta familia tenemos a los productos de Fortinet, SonicWALL, WatchGuard, Nortel, Cisco, Linksys, Netscreen (Juniper Networks), Symantec, Nokia, U.S. Robotics, D-link, Mikrotik, etc.

Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de interoperatividad en los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general.

Ventajas

Integridad, confidencialidad y seguridad de datos.
Las VPN reducen los costos y son sencillas de usar.
Facilita la comunicación entre dos usuarios en lugares distantes.

Tipos de VPN

VPN de acceso remoto

VPN punto a punto

Tunneling

VPN over LAN

NAT

Network address translation

mecanismo utilizado por Routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

BIBLIOGRAFÍA

COBIT INFORMATION SYSTEMS SECURITY a Practioner's referencie –
Martín P. J. Krats PHILIP FITES VAN NOSTRAD REINHOLD
isbn 0-442-00180-0 .
Jung José Nombela Paraninfo SEGURIDAD INFORMÁTICA
ISBN: 84-283-2341-0

UNIDAD ACADÉMICA PROFESIONAL TIANGUISTENCO

PROGRAMA EDUCATIVO:
INGENIERÍA EN SOFTWARE

OCTAVO SEMESTRE

UNIDAD DE APRENDIZAJE:
SEGURIDAD INFORMÁTICA

TIPOS DE VIRUS, VPN, MATRIZ DE RIESGOS

ELABORADO POR: L. CID MARTIN GARCIA AVILA

UTILIZACIÓN DEL MATERIAL

SEGURIDAD INFORMÁTICA

1. Introducción a la Seguridad Informática

OBJETIVO

Que el alumno capte los conceptos básicos que constituyen el eje de los desarrollos y aprecie la diferencia entre ellos y los respectivos alcances e implicaciones desde la perspectiva de la administración de Riesgos; Controles y Seguridad en ambientes computarizados. Que sea capaz de identificar y comprender las condiciones de vulnerabilidad de los activos informáticos.

VPN

NAT

Técnicas para asegurar el sistema

Técnicas de desarrollo
Medidas de seguridad físicas
Codificar la información
Contraseñas difíciles de averiguar
Vigilancia de red
Redes perimetrales de seguridad, o DMZ
Tecnologías repelentes o protectoras
Actualizaciones
Copias de seguridad
Controlar el acceso a la información
Restringir el acceso

BIBLIOGRAFÍA

PROGRAMA

OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

Conocer los elementos operativos requeridos para la transmisión y recepción de información.
Identificar los elementos de seguridad informática en aspectos de físicos y lógicos así como redes de computo, además de medidas de recuperación de información.
Analizar los diversos métodos para garantizar la seguridad y confiabilidad de los datos que circulan en las redes, asegurando
el libre tránsito de información y manteniendo las condiciones de privacidad definidas por los usuarios y los administradores de los sistemas.

1.4 POSIBLES RIESGOS

RIESGO
Es una medida cuantitativa de la importancia de un incidente que es mayor, cuanto mayor es su impacto y probabilidad.

VULNERABILIDAD
La evaluación objetiva de la probabilidad de sufrir un determinado ataque en un plazo de tiempo dado.

DEBILIDAD
OPORTUNIDAD