FUNDAMENTOS DE SEGURIDAD INFORMÁTICA

Ricardo López

EJE 4

Propongamos

Fuente: shutterstock.com/188832089

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED
ILUMNO

ÍNDICE

INTRODUCCIÓN

¿A qué amenazas se ven expuestos los sistemas informáticos y cómo se pueden minimizar sus posibles efectos?

En este último eje del conocimiento se estudiarán los diferentes tipos de amenazas que pueden afectar un sistema informático y la forma de brindar la protección eficiente y eficaz a la organización y/o empresa, y de minimizar y/o mitigar el impacto del incidente de seguridad.

Para lograr los objetivos propuestos en el eje, nos apoyaremos en lecturas complementarias, video cápsulas, video relatos, talleres, y otras actividades pedagógicas que complementarán el desarrollo de dicho eje.

Los invito a desarrollar todas y cada una de las actividades propuestas.

Introducción a las amenazas de seguridad informática

Video

Como elemento introductorio los invito a ver la video cápsula "Seguridad informática", la cual explica las principales amenazas a las que está expuesta la información.

Seguridad Informática

https://www.youtube.com/watch?v=Nxns7cqfMsg&t=89s

El uso y crecimiento del entorno de las TIC dentro de organizaciones públicas y/o privadas, conduce a diversas incertidumbres y riesgos frecuentes, a los que se encuentra sometida la información y los dispositivos que la contienen, teniendo que enfrentarse con una gran variedad de amenazas y vulnerabilidades asociadas a estos entornos informáticos, razón por la cual se deben gestionar, monitorear y controlar dichos sistemas para ofrecer un óptimo servicio.

Al no desarrollar planes y políticas de seguridad acordes a las necesidades de la compañía, generará riesgo de sucesos inesperados que irán en detrimento de la misma, causando efectos negativos y no deseados de tipos económicos, financieros, sociales, pérdida de la reputación, competitividad, pérdidas de oportunidades y/o confianza, entre otros, sus clientes internos y externos, pudiendo llevarla hasta el cierre definitivo de la misma.

¡Recordemos que!

Las vulnerabilidades indican una debilidad en la tecnología o procesos relacionados con la información, propios de la infraestructura tecnológica que la contiene y/o los procesos que se generan.

La amenaza por su parte, resulta a causa de cualquier evento o situación que pueda afectar el desarrollo de las actividades dentro de la organización, estas, toman ventaja de las vulnerabilidades que se presentan en la compañía y se pueden generar desde cualquier entorno de la misma, la amenaza tiene el potencial de causar daño a la compañía y/o a los activos de la misma.

Figura 1. Vulnerabilidad informática
Fuente: shutterstock.com/545167099

Los sistemas informáticos como se ha mencionado son vulnerables por estar expuestos a múltiples amenazas que pueden provocar diferentes daños y que generarán pérdidas significativas dentro de una organización. Para impedir y/o mitigar estas amenazas se debe realizar el análisis del riesgo informático, resultado del cual se podrán implementar controles de seguridad adecuados, estrategias y políticas de seguridad que minimizarán el impacto de cualquier amenaza.

Este análisis de riesgos es un proceso que permite identificar en el grado de exposición de los activos informáticos, así como detectar sus vulnerabilidades y amenazas, de igual forma, esta evaluación determina su probabilidad de ocurrencia y el impacto de las mismas, para así poder implementar los controles adecuados en el que se busca aceptar, disminuir, transferir o evitar los riesgos.

El ministerio de TIC en la guía 7 "Guía de gestión del riesgo", describe las amenazas más comunes a las que se ve expuesta la información y los sistemas que la contienen, así mismo, desarrolla una serie de lineamientos que permitan mitigar los riesgos.

Lectura recomendada

Para mayor comprensión de los temas los invito a realizar la lectura de la Guía de Gestión del Riesgo, la cual da lineamientos para la gestión de amenazas y describe las principales amenazas a las que está expuesta la información.

Guía número 7 "Guía de Gestión del Riesgo"

Ministerio de Tecnologías de la Información y las Comunicaciones

TIPO	AMENAZA
Daño físico.	Fuego.
	Agua.
	Contaminación.
	Accidente importante.
	Destrucción de equipo o medios.
	Polvo, corrosión, congelamiento.
Eventos naturales.	Fenómenos climáticos.
	Fenómenos sísmicos.
	Fenómenos volcánicos.
	Fenómenos meteorológicos.
	Inundaciones.
Pérdida de los servicios esenciales.	Fallas en el sistema de suministro de agua o aire acondicionado.
	Pérdida del suministro de energía.
	Falla en equipo de telecomunicaciones.
Perturbación debida a la radiación.	Radiación electromagnética.
	Radiación térmica.
	Impulsos electromagnéticos.
Compromiso de la información.	Interceptación de señales de interferencia comprometida.
	Espionaje remoto.
	Escucha encubierta.
	Hurto de medios o documentos.
	Hurto de equipos.
	Recuperación de medios reciclados o desechados.
	Divulgación.
	Datos provenientes de fuentes no confiables.
	Manipulación con hardware.
	Manipulación con software.
	Detección de la posición.
Fallas técnicas.	Fallas del equipo.
	Mal funcionamiento del equipo.
	Saturación del sistema de información.
	Mal funcionamiento del software.
	Incumplimiento en el mantenimiento del sistema de información.
Acciones no autorizadas.	Uso no autorizado del equipo.
	Copia fraudulenta del software.
	Uso de software falso o copiado.
	Corrupción de los datos.
	Procesamiento ilegal de datos.
Compromiso de las funciones.	Error en el uso.
	Abuso de derechos.
	Falsificación de derechos.
	Negación de acciones.
	Incumplimiento en la disponibilidad del personal.

Tabla 1. Principales amenazas a los sistemas informáticos y la información
Fuente: Guía 7 - Gestión de riesgos Min TIC

Amenazas físicas y lógicas

Video

Para introducirnos en el tema los invito a ver la video cápsula "Centro Cibernético de la Policía Nacional", en el cual se explican las principales amenazas, los principales delitos y se generan recomendaciones de seguridad.

Centro Cibernético de la Policía Nacional

https://www.youtube.com/watch?v=bM8OUkryTeg

Las amenazas físicas abarcan los daños o errores de hardware (equipos terminales, equipos intermediarios, medios de transmisión).

Las amenazas lógicas engloban todo el daño y errores que puede ocurrir en el software, filtración, manipulación, corrupción de los archivos, entre otros.

Amenazas	Categoría	Descripción
Físicas	Fallos en los dispositivos terminales, dispositivos intermediarios y/o el cableado o medio de conexión.	Fallo en discos duros, memorias, procesadores, fuentes de poder, etc. Cableado defectuoso. Red de energía defectuosa. Fallo en router, switch, bridge.
Lógicas	Software malicioso.	Intrusos y ataques en la red. Malware. Backdoors. Virus informáticos.
	Software defectuoso.	Bugs o Buffers.

Tabla: 2. Amenazas físicas y lógicas
Fuente: propia

Amenazas según su origen

En esta clasificación se analiza el origen o procedencia de la amenaza y se pueden resumir en: naturales, de agentes externos y de agente internos:

Amenazas	Categoría	Descripción
Naturales	Ocasionado por la naturaleza.	Inundación. Incendio. Tormenta. Fallas eléctricas. Huracanes. Terremotos.
Agentes externos	Personas	Malwares. Virus informáticos. Sabotajes terroristas. Ataques e intrusiones de criminales. Secuestro de información.
Agentes internos	Personas	Descuidos de empleados Errores en la utilización de herramientas. Mal uso de los recursos. Mala intención por parte del empleado.

Tabla: 3. Amenazas según su origen
Fuente: propia

Amenazas según su intención

Este tipo de amenaza se produce mediante: accidentes, errores, actualizaciones malintencionadas.

Amenazas	Descripción
Accidentes	Averías en hardware. Fallos en el Software. Naturales.
Errores	Mal uso de herramientas. Explotación. De ejecución.
Actuaciones malintencionadas	Sabotajes. Intentos de intrusión. Robos. Fraudes.

Tabla: 4. Amenazas según su origen
Fuente: propia

Amenazas según su naturaleza

Esta clasificación se genera debido a la naturaleza y al factor de seguridad que compromete la información, generada por personas no autorizadas como: intercepción, modificación, interrupción y fabricación.

Amenazas	Descripción
Intercepción de datos	Uso de privilegios no adquiridos. Copias ilícitas de programas o datos. Escuchas en la comunicación de datos.
Modificación	Alteración para su beneficio. Modificación de bases de datos. Modificación de elementos en el hardware.
Interrupción	Deja no utilizable o no disponible un elemento o todo el sistema. Destrucción del hardware. Borrado de programas y/o datos. Fallos en el S.O.
Fabricación	Delitos de falsificación. Añadir transacciones en red. Añadir registros en bases de datos.

Tabla 5. Amenazas según su origen
Fuente: propia

Amenazas según los tipos de atacantes

La clasificación se produce debido a los tipos o caracterización de atacantes que existen, es decir, las personas que llevan a cabo los ataques hacia un sistema informático.

Amenazas	Descripción
Hackers	Experto o con grandes conocimientos en el área de informática, se vanaglorian y se consideran a sí mismos ágiles en romper la seguridad de un sistema informático, conocido como sombrero blanco. Los motiva el reto, el ego, el estatus, la religión, entre otras motivaciones. El hacker no es un delincuente como se ha querido hacer ver, ya que en el momento que una persona de estas características saca beneficios económicos se considera un criminal de la computación y no un hacker.
Crackers	Persona que desarrolla los Crack es decir programas que permiten acceder de forma libre a software licenciado, vulnerando la seguridad y la integridad del mismo y atentando contra los recursos económicos de la persona o empresa que lo desarrollo. Esta práctica se considera un delito informático penalizado por la Ley 1273 de 2009. En el mundo informático se les ve como Robín Hood.
Phreakers	Personas dedicadas al estudio y comprensión del funcionamiento de los teléfonos, que aplicando técnicas hacker realizan actividades no autorizadas como escucha de llamadas, interceptación de las mismas, ejecución de llamadas si costo, entre otras actividades. La actividad se conoce comúnmente como “Chuza” y se considera un delito informático penalizado por la Ley 1273 de 2009.

Lammers	Persona que presume de sus pocos conocimientos por conocer o manejar una herramienta y se considera hacker, pero no lo es.
Ciber terrorista	Criminales expertos en informática, se dedican a chantajear, destruir, atemorizar y generar pánico por medio de las redes. Generan ataque de denegación de servicios DDOS, manipulación de sistemas, penetración al sistema, guerra de información entre otros. Se considera delito informático y es penalizado por la Ley 1273 de 2009.
Criminal de la computación	Persona con avanzados conocimientos informáticos y de seguridad, trabaja en descubrir vulnerabilidades de los sistemas y/o redes para obtener beneficios propios en detrimento de las demás personas y/o empresas (se le conoce como sombrero negro). Utiliza software denominado crimeware para delitos financieros. Esta actividad es considerada delito informático y es penalizada por la Ley 1273 de 2009. Dentro de estas actividades encontramos el fraude, soborno, suplantación, intrusión, alteración, divulgación, entre otros.
Newbie	Aquel que está empezando en el tema de hacking, es decir un hacker novato.
Programadores de virus	Considerados expertos en lenguajes de programación, redes y sistemas, el cual crean programas de carácter dañino para que afecten las aplicaciones o sistemas informáticos.
Carders	Se dedican a atacar las vulnerabilidades de tarjetas crédito o débito y/o cajeros electrónicos.
Sniffers	Expertos que analizan el tráfico de las redes para obtener información que son transmitidos por la red, con ayuda de programas llamados sniffer.

Tabla 6. Amenazas según tipo de atacante
Fuente: propia

Amenazas según los tipos de ataques

Video

Como elemento introductorio a las amenazas según el tipo de ataque, los invito a ver la video cápsula "tipos de amenazas - Malware", la cual nos describe los principales tipos de malwares y sus características.

Tipos de amenaza - Malware

https://www.youtube.com/watch?v=xApsVQVcuKo

Esta clasificación abarca los tipos de ataques que pueden realizarse en un sistema informático, dada la caracterización del tipo de atacante.

Amenazas	Descripción
Spoofing	Son técnicas utilizadas para suplantar la identidad de algún sistema informático. Los ataque más comunes son: IP Spoofing (suplantación de dirección IP), DNS Spoofing (suplantación de DNS), Arp Spoofing, web Spoofing, entre otros.
Sniffing	Realiza la monitorización y análisis del tráfico de una red para obtener información (captura de tramas).
Conexión no autorizada	Backdoors o puertas traseras que son dados por los agujeros de seguridad de un equipo de cómputo (host o servidor) en la cual realiza una conexión no autorizado a los mismos.
Malware	Software malintencionado con diversos objetivos como causar daño, abrir puertos, consumirse los recursos de red o del equipo, publicidad, afectar el buen funcionamiento de un dispositivo, entre otros.
Gusano - worm	Malware informático con la capacidad de auto reproducirse, el objetivo es consumir los recursos de la red y/o la máquina, no requiere intervención del usuario, su método de propagación preferido son redes P2P (Emule, Ares, BitTorrent, entre otros).
Troyano	Malware informático diseñado para abrir puertos y permitir tomar el control remoto de la máquina, se presenta como algo inofensivo, requiere la intervención del usuario.

Virus	Malware informático diseñado para causar daño a la información y/o a los equipos que la contienen, eliminando, alterando, reescribiendo, modificando la información. Tiene la capacidad de infectar otros archivos, y puede presentarse como un troyano u otro tipo de malware.
Keyloggers	Software malintencionado que captura todo lo que el usuario escribe (capturador de pulsaciones de teclado), o puede capturas de pantallas para obtener claves de acceso, y demás datos.
Spam	Considerado como correo o mensajes basura, no deseados o fuentes desconocidas.
Denegación de servicio	Afecta la operatividad de un sistema interrumpiendo su servicio. Puede ser una red, un servidor, un equipo intermediario (router, switch, AP) o algún servicio, se conocen como ataque DDoS.
Ingeniería social	Personas que manipulan a personas u organizaciones para obtener información confidencial, tales como encuestadores, delincuentes, investigadores privados.
Phishing	Suplantación de identidad de una página web o de un organismo, engaña al usuario para obtener información confidencial. Ejemplo: robo de información bancaria de una persona.
Pharming	Redirección de un nombre de dominio DNS hacia otra máquina distinta que es falsa y fraudulenta para obtener información confidencial.
Password cracking	Se emplea el espionaje directo, es decir mirando lo que hace un usuario sin que este lo note, detentando la digitación de credenciales o realizando ataques de fuerza bruta.
Bonnets	Conjuntos o red de robots informáticos, que se ejecutan de manera automática y en múltiples hosts de diferentes lugares, para controlar ordenadores/servidores de forma remota, comúnmente se utilizan para ataque de DDoS.
Ransomware	Programas dañinos que restringen el acceso a la información, la encriptan y luego piden rescate por esta.

Tabla: 7. Amenazas según tipo de ataque
Fuente: propia

Video

Para afianzar los conocimientos los invito a ver el video relato "Creación de Malware", en el cual explico de forma práctica y de manera pedagógica como crear un malware.

Video Relato creación de malware

https://vimeo.com/244855566

Recuerden que desarrollar malware es un delito tipificado por la Ley 1273 de 2009, los ejercicios propuestos y desarrollados en este módulo son de carácter pedagógico y para comprender las amenazas a la que está expuesta la información y los sistemas informáticos.

Lectura recomendada

Ahora los invito a desarrollar la lectura de la Ley 1273 de 2009.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Congreso de la República

Riesgos

Se puede considerar el riesgo como un valor relativo, probable en términos de pérdidas de toda índole, en un lugar específico vulnerable a una amenaza particular. Esto quiere decir que el riesgo es toda probabilidad de que ocurra un hecho y conlleve a producir ciertos efectos, se determinan por la probabilidad de ocurrencia de un evento y la magnitud del impacto que genere o cause.

Riesgo = Amenaza x Vulnerabilidad

Los eventos son aquellas acciones que se desarrollan en la red o sistema, algunos ejemplos son: intentos de conexiones, respuesta exitosa de una url, respuesta enviada por un servidor a una petición hecha en el navegador, conexión entre dos hosts, una autenticación y login entre otros.

Figura 2. Riesgo
Fuente: shutterstock.com/317273255

Lectura recomendada

Ahora, para conocer sobre la gestión y clasificación de las amenazas a las que se ve expuesta la información, realice la lectura de la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones

Política de seguridad

La política de seguridad son normas, lineamientos, reglas de buenas prácticas para mantener la seguridad de los sistemas informáticos y la información.

Para definir una política de seguridad de un sistema informático, se debe generar cuatro etapas:

1. *Definir las necesidades:* levantamiento de inventario de los activos de la organización y determinación de vulnerabilidades y amenazas de cada uno de dichos activos (generación de matriz del riesgo).

2. *Diseño e implementación de política de seguridad:* en esta etapa determina los diferentes métodos y/o mecanismos diseñados para asegurar el sistema informático, definir el problema, el alcance, los objetivos, los requerimientos (técnicos, económicos, humanos, etc...), las sanciones, y todos los demás elementos necesarios para el desarrollo e implementación de una política de seguridad.

3. *Realizar auditorías de seguridad:* seguimiento y evaluación de las medidas de protección que se tienen implementadas y adoptadas en el diseño de las políticas de seguridad, se conoce también a esta fase como la detección de incidentes de seguridad, por lo general se contrata actores externos para su realización (auditoría de sistemas externa).

4. *Definición de acciones:* cuando se detecta una nueva vulnerabilidad y/o amenaza el resultado es la implementación de una nueva política de seguridad, y/o actualización de una política existente, ya que de esta forma se prevé y planifica las medidas que han de tomarse cuando se presente algún incidente de seguridad, estas acciones en busca de la mejora continua optimizar el proceso de gestión de seguridad de la información y el proceso de gestión del riesgo y están alineadas con el ciclo de mejora continua PHVA.

Instrucción

Para una mejor apropiación de los aprendizajes lo invitamos a realizar a realizar la actividad sopa de letras.

Matriz para la evaluación o análisis del riesgo

El análisis del riesgo es un trabajo muy extenso y que requiere tiempo para obtener muy buenos resultados, pero es necesario realizarlo al detalle, ya que permite visualizar los posibles daños a los que están expuestos los recursos tecnológicos y tomar acciones que permitan minimizar dichas vulnerabilidades, una vez desarrollado el análisis de seguridad es importante clasificar y priorizar los riesgos a los que se está expuesto y proceder a desarrollar una política de seguridad para cada riesgo detectado.

En muchas organizaciones pasan por alto este importante eslabón, ya que no se cuenta con el personal técnico, los equipos de cómputo necesarios, los recursos económicos, ni con el tiempo para dedicarlos a la seguridad de la información.

Matriz de riesgo

La matriz de riesgo consiste en el método de análisis de los riesgos, representado con un gráfico de riesgo, que emplea la fórmula:

Riesgo = (amenaza x vulnerabilidad) vs. impacto o magnitud de daño

Estos últimos darán valores cuantitativos y luego se realiza sus correspondientes análisis cualitativos:

La escala, como se podría desarrollar la matriz de riesgos es:

1. Insignificante (ninguna).

2. Baja.

3. Mediana.

4. Alta.

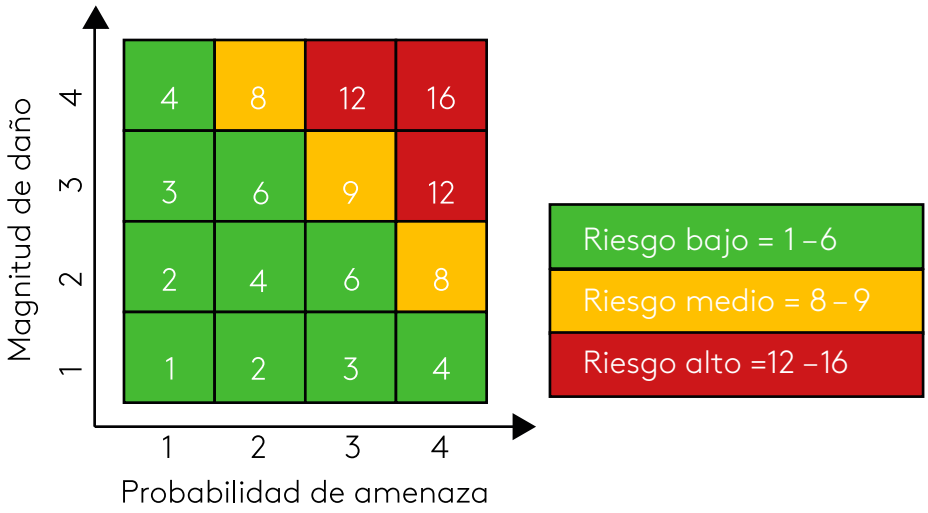

Figura 3. Escala de matriz de análisis de riesgo
Fuente: propia

Existen diversas matrices propuestas para el análisis de riesgos, se recomienda indagar al respecto y adecuar la que considere de mayor aporte para la gestión del riesgo.

Instrucción

Los invito a revisar la matriz de análisis de riesgo que se presenta como material de apoyo en la carpeta de recursos.

Por otra parte, recomiendo para el desarrollo de una política de seguridad y gestión del riesgo apoyarse en los documentos.

- Guía 7 de Min Tic Colombia, para verificar la propuesta de matriz análisis de amenazas, vulnerabilidades y riesgo para entidades del estado. (válidas para cualquier tipo de empresa privada o pública).
- ISO/IEC 27001:2005 /2013 Sistema de gestión de la seguridad de la información SGSI, la cual genera lineamientos para la creación de políticas de seguridad y gestión de la seguridad de la información.
- ISO/IEC 27005:2008 Gestión de riesgos, la cual proporciona directrices para la gestión del riesgo de la seguridad de la información y define los conceptos, terminología, modelo y procesospara una adecuada gestión de riesgos.

Lectura recomendada

Antes de finalizar y para reafirmar los conocimientos adquiridos hasta el momento los invito a realizar la siguiente lectura.

Amenazas y vulnerabilidades de la seguridad informática.

César Tarazona

A modo de síntesis observemos el siguiente organizador gráfico.

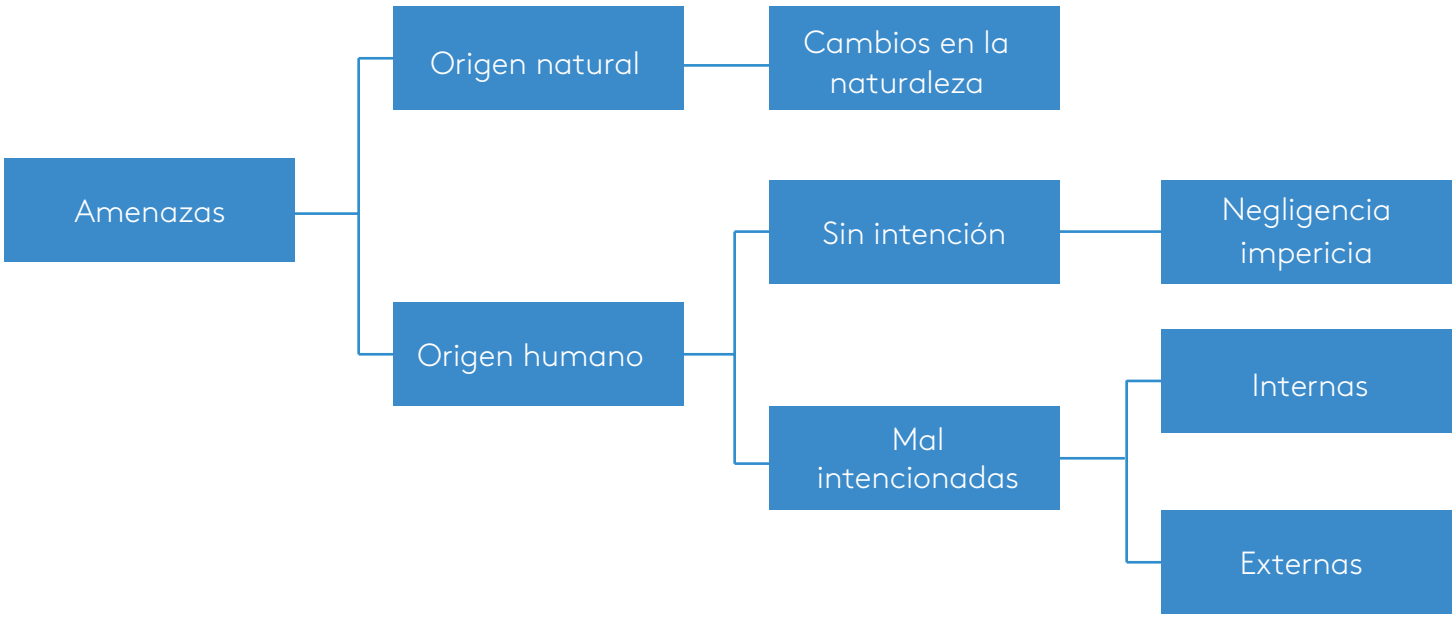

Figura 4. Tipos de amenazas
Fuente: propia

Video

Como resumen del eje 4 los invito a ver la Videocápsula "Delitos Informáticos - CTI" la cual explica los principales riesgos y amenazas a las que está expuesta la información.

Delitos informáticos CTI

https://www.youtube.com/watch?v=prBN0jYN0uo

Instrucción

Para finalizar los invito a desarrollar de forma colaborativa la evaluación final del curso.

BIBLIOGRAFÍA

Álvarez, M. y Pérez, G. (2004). *Seguridad informática para empresas y particulares*. Madrid: McGraw-Hill

Austin, R. y Darby, C. (2004). *El mito de la seguridad informática*. Madrid: Ediciones Deusto - Planeta de Agostini Profesional y Formación S.L.

Baca, U. G. (2016). *Introducción a la seguridad informática*. México: Grupo Editorial Patria.

Chicano, T. (2014). *Gestión de incidentes de seguridad informática (MF0488_3)*. Madrid: IC Editorial.

Chicano, T. (2014). *Auditoría de seguridad informática (MF0487_3)*. Madrid: IC Editorial.

Costas, S. J. (2014). *Seguridad informática*. Madrid: RA-MA Editorial.

Costas, S. (2014). *Mantenimiento de la seguridad en sistemas informáticos*. Madrid: RA-MA Editorial.

Escrivá, G., Romero, S. y Ramada, D. (2013). *Seguridad informática*. Madrid: Macmillan Iberia, S.A.

Ficarra, F. (2006). Antivirus y seguridad informática: el nuevo. *Revista Latinoamericana de Comunicación CHASQUI*.

Giménez, A. J. F. (2014). *Seguridad en equipos informáticos (MF0486_3)*. Madrid: IC Editorial.

Gómez, F. y Fernández, R. (2015). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad*. Madrid: AENOR - Asociación Española de Normalización y Certificación.

Gómez, V. (2014). *Auditoría de seguridad informática*. Madrid: RA-MA Editorial.

Gómez, V. (2014). *Gestión de incidentes de seguridad informática*. Madrid: RA-MA Editorial.

Hernández, E. (2016). *La criptografía*. Madrid: Editorial CSIC Consejo Superior de Investigaciones Científicas.

BIBLIOGRAFÍA

Lamadrid, V., Méndez, G. y Díaz, H. (2009). *CERT-MES: sitio Web de seguridad informática para REDUNIV*. La Habana: Editorial Universitaria.

McClure, S., Scambray, J. y Kurtz, G. (2010). *Hackers 6: secretos y soluciones de seguridad en redes*. México: McGraw-Hill Interamericana.

Molina, M. (2000). *Seguridad de la información. Criptología*. Córdoba: El Cid Editor.

Paredes, F. (2009). *Hacking*. Córdoba: El Cid Editor | apuntes.

UNED. (2014). *Procesos y herramientas para la seguridad de redes*. Madrid: Universidad Nacional de Educación a Distancia.

Roa, B. (2013). *Seguridad informática*. Madrid: McGraw-Hill

Sanz, M. (2008). *Seguridad en linux: guía práctica*. Madrid: Editorial Universidad Autónoma de Madrid.

Zayas, D. y Sánchez, R. (2010). *Sistema de apoyo al entrenamiento en seguridad informática: SEGURIN*. La Habana: Editorial Universitaria.