FUNDAMENTOS DE SEGURIDAD INFORMÁTICA

Ricardo López

EJE 3

Pongamos en práctica

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED
ILUMNO

Fuente: shutterstock/340334438

ÍNDICE

Introducción 3

Introducción vulnerabilidades informáticas 4

Vulnerabilidades de un sistema informático 7

Según los recursos 8

Otros factores 9

¿Cómo proteger el sistema informático de riesgos a causa de vulnerabilidades? 11

Bibliografía 20

INTRODUCCIÓN

¿Cómo se pueden detectar las vulnerabilidades en los sistemas informáticos?

La vulnerabilidad de un sistema informático se visualiza como la debilidad del sistema, la cual por sí sola no causa daño, pero permite o pone en riesgo el sistema admitiendo que una amenaza actúe sobre este.

La detección y realización de un análisis de vulnerabilidades mediante el cual se determine el nivel de exposición de los activos o elementos informáticos funcionales y de importancia dentro de la organización, conlleva a tomar diversas medidas de mitigación y protección, consideradas como buenas prácticas, evitando que su impacto y costo se vean afectados circunstancialmente.

En este tercer eje del conocimiento se estudiarán las vulnerabilidades de un sistema informático según los recursos y la función, se trabajará sobre la seguridad en redes Wi-Fi, definiendo y configurando de forma práctica el control de acceso y la seguridad de la información en dichas redes.

El marco metodológico de este eje es teórico–práctico, donde el estudiante a partir de los conceptos, generará análisis, implementará soluciones y propondrá nuevas alternativas de mejora.

Para conseguir los objetivos de este eje y afianzar los conocimientos, nos apoyamos en video cápsulas, video relatos, lecturas complementarias, talleres, entre otros recursos de aprendizaje.

Introducción vulnerabilidades informáticas

Video

Para dar inicio a este eje los invito a ver la video cápsula "Conceptos de vulnerabilidad, riesgo y amenaza" la cual explica cada uno de estos conceptos.

Conceptos de amenaza, riesgo y vulnerabilidad.

https://www.youtube.com/watch?v=9hJ4fgfePfg

Como ya se ha mencionado, las vulnerabilidades en conceptos de informática, son una debilidad o falla que se presenta en un entorno de operación tecnológico, que son producidos por un elemento o todo un sistema informático, que expone en el grado de riesgo la seguridad de la información, puede llegar a comprometer y afectar la integridad, la disponibilidad y/o la confidencialidad de la información, por lo que es necesario acudir a mecanismos de detección y eliminación de esos posibles riesgos a los que están sometidos.

La vulnerabilidad es el elemento que permite que una amenaza se plasme, en otras palabras, algo que no hacemos o estamos haciendo mal.

Ejemplo

La no instalación de actualizaciones o parches de seguridad, la carencia de software antivirus o la no actualización del mismo, la no configuración de firewall, entre otros muchos factores predecibles y controlables.

Firewall

Firewall o cortafuegos. Dispositivo o software de seguridad.

Por otra parte, la amenaza hace referencia al hecho, interno o externo, que puede afectar los pilares de la seguridad (confidencialidad, disponibilidad y/o integridad de la información), ejemplo, un ataque de denegación de servicios (DDoS), desastres naturales como, terremotos, inundaciones, huracanes, entre otros.

El riesgo por su parte es la consecuencia que conlleva a la pérdida de continuidad o la vulneración de la seguridad, por ejemplo, robo de información, corte del servicio, entre otros.

En otras palabras, evaluar el riesgo es el producto de las amenazas por las vulnerabilidades en relación con la capacidad de respuesta o de autogestión de la organización que pueden dirigirse positivamente a la gestión de riesgo, gráficamente:

$$\text{Riesgo} = \frac{\text{Amenaza x Vulnerabilidad}}{\text{Capacidad de reacción}}$$

El riesgo y la vulnerabilidad preexistentes se expresan de forma indiscutible en la manifiesta búsqueda de una estrategia de desarrollo basada en procesos que implican como componente fundamental, la reducción de la vulnerabilidad existente.

Como se muestra en la siguiente imagen, el riesgo depende entonces de la probabilidad de ocurrencia de que una determinada amenaza se materialice, aprovechando una vulnerabilidad (debilidad) y está a la vez produce un daño o impa o. El producto de estos factores representa el riesgo.

DDoS

Ataque de denegación de servicio, que atenta contra la disponibilidad del sistema.

Continuidad

La continuidad hace referencia a la característica de mantener el servicio activo ante cualquier eventualidad.

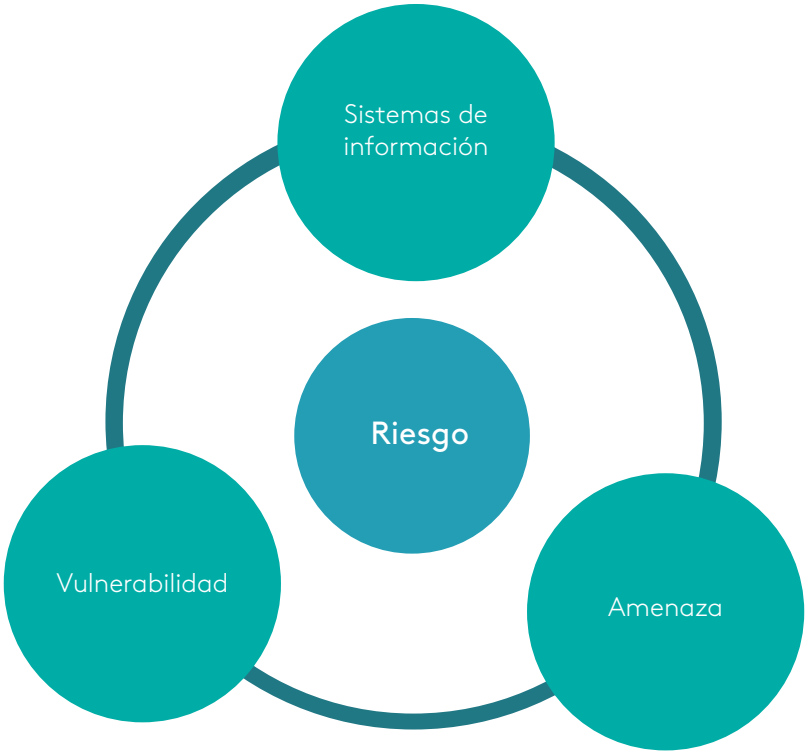

Figura 1. Relación entre vulnerabilidad y amenaza frente a los riesgos de un SI.
Fuente: propia

Vulnerabilidades de un sistema informático

Lectura recomendada

Para tener una visión inicial de las vulnerabilidades informáticas los invito a realizar la lectura complementaria del capítulo 11 de la guía No.7 de MinTic - Gestión del riesgo.

Guía de gestión de riesgos. Seguridad y privacidad de la información. Guía No.7

MinTic

Según los recursos

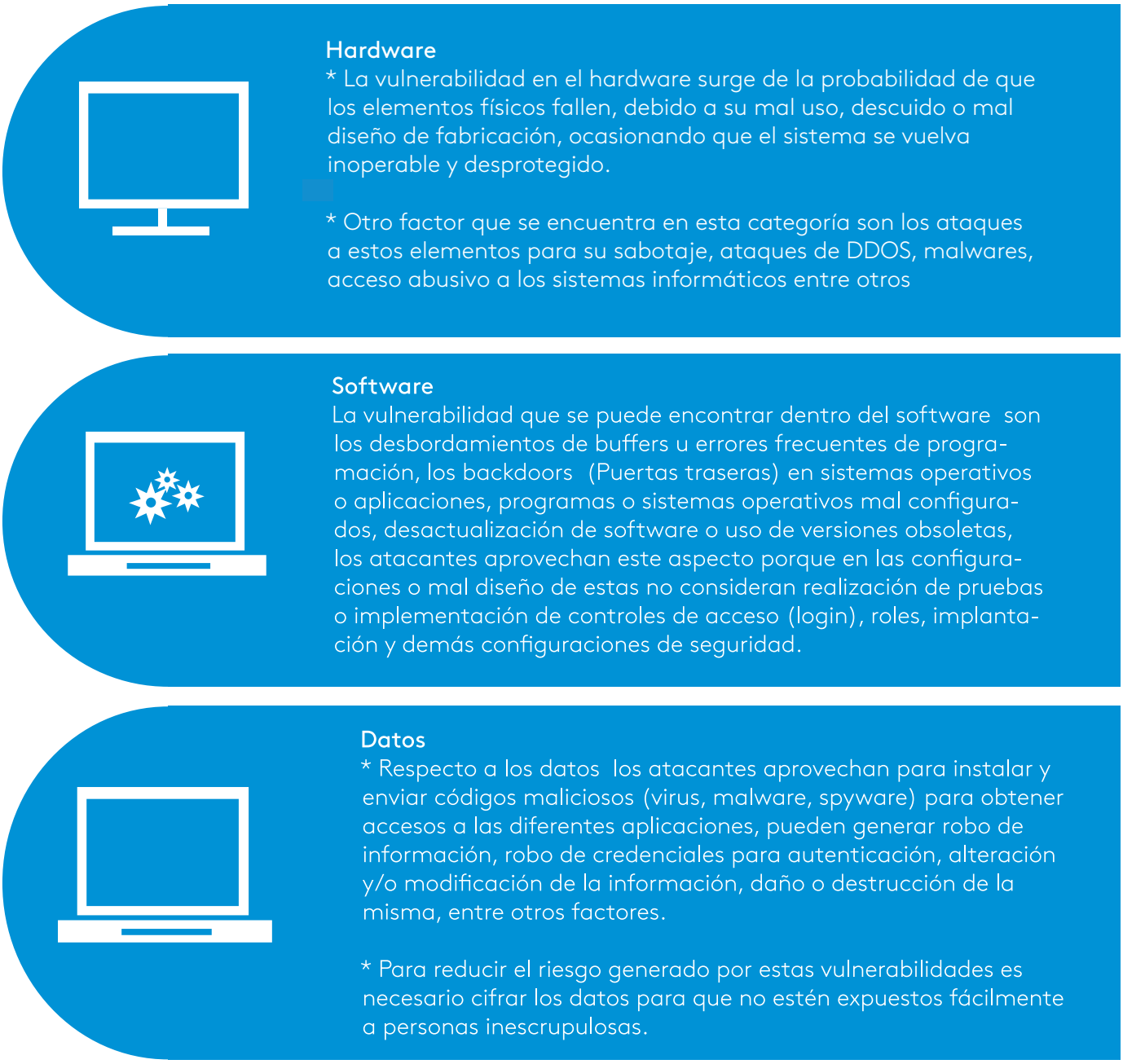

Figura 2. Vulnerabilidades según los recursos
Fuente: propia

Otros factores

- *Causas naturales:* son las que concierne a los desastres naturales, que causan daño al sistema informático, son ocasionadas principalmente en las deficiencias o malas medidas tomadas para enfrentar los desastres como incendios, exposición de algún elemento al agua, cortos, tormentas eléctricas o calor, ejemplo, un mal sistema de ventilación o regulación de la temperatura, el no uso de UPS, de breaks o interruptores para picos de voltajes, el no uso de sensores, la no redundancia de discos, entre otros muchos factores que pueden minimizar el impacto de un desastre.

- *Causas físicas:* son aquellas que están relacionadas con el acceso físico del sistema informático y del lugar donde se encuentran los elementos o equipos de cómputo dentro de las instalaciones.

  La mala ubicación o aseguramiento de los equipos o elementos de cómputo donde se guarda la información sensible o que hacen parte de procesos esenciales del sistema, la falta de medidas de control de acceso a los centros de cómputo, rack, gabinetes, servidores, entre otros, generadas por malas prácticas de políticas de acceso de los empleados o usuarios a los sistemas informáticos.

- *Causas de red:* son aquellas que por mala implementación no se tiene control de aseguramiento de los elementos que conforma el sistema informático y que emplean las redes de datos para acceder a estos recursos.

  Es un aspecto muy susceptible con la intercepción de la información, al tratarse de una serie de equipos interconectados entre sí, el mal aseguramiento de estos canales compartiendo los recursos y tráfico que circulan dentro de la red, originan ataques a la totalidad de la misma.

  No llevar un control de quienes se conectan o identificar quien está en su red de usuarios no autorizados, puede llegar a ocasionar fallas de denegación de servicio, combinando las anteriores vulnerabilidades descritas.

- *Causas de factor humano:* es uno de los aspectos más importantes y difíciles de controlar, debido a que se da por la negligencia en el seguimiento de políticas o procesos de seguridad, el mal uso de los elementos o equipos informáticos, los convierte en amanezcas constantes y una de las partes más vulnerables de los sistemas informáticos.

  Este aspecto puede darse o puede deberse a una mala capacitación, concientización y cultura corporativa, factores que conlleva al ser humano a cometer errores o someter un sistema, otro factores como el resentimiento, falta de ética, poca lealtad con la organización, generan una brecha de inseguridad altísima ya que el usuario conoce la información, sabe cuál es la importancia de esta, conoce a quien le sirve y/o para qué sirve y tienen acceso a la misma, pudiendo generar robo, venta o destrucción de la información.

Según su función las vulnerabilidades se pueden generar por:

Grupo	Definición
Diseño	Mal diseño de las redes de datos, diseño plano de redes (sin jerarquía), varios servicios sobre los mismos canales, dispositivos intermediarios switch y router sin seguridad habilitada, redes inalámbricas con acceso por defecto, configuración deficiente de políticas de seguridad establecidas.
Implementación	Buffers u overflows en las aplicaciones desarrolladas, se produce cuando un programa no controla la cantidad de datos que se copian en buffer, de forma que si esa cantidad es superior a la capacidad del buffer los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original. Se puede aprovechar para ejecutar códigos que nos den privilegios de administrador. Instalar e implementar software ilegal, sin soporte, ni actualizaciones. No implementación de parches de seguridad. No contar con el soporte de los fabricantes. No implementar elementos de seguridad como antivirus, firewall, entre otros. Mantener desactualizado los sistemas de seguridad.
Uso	Mal uso o manejo de los sistemas informáticos asignados a usuarios. Mala configuración de los sistemas. Falta de capacitación a los usuarios y responsables de TI sobre manejo o fallas de los sistemas informáticos. Carencia de recursos de seguridad en TI. Disponibilidad de herramientas que facilitan los ataques. Limitación gubernamental de tecnologías de seguridad.
Vulnerabilidad día cero	Son considerados ataques contra las aplicaciones que ejecutan códigos maliciosos en las vulnerabilidades detectadas en los sistemas y son desconocidas por los usuarios y fabricantes. Cuando no exista una solución "conocida" para una vulnerabilidad, pero si se conoce como explotarla, entonces se le conoce como "vulnerabilidad 0 days".

Tabla: 1. Vulnerabilidades según su función
Fuente: propia

Figura: 3. Seguridad informática
Fuente: shutterstock.com/127894739

¿Cómo proteger el sistema informático de riesgos a causa de vulnerabilidades?

Para proteger la información y los sistemas que la contienen se recomienda:

- Desarrollar inventario de activos y dispositivos informáticos, elaborando análisis de vulnerabilidades para cada activo y/o dispositivo de la empresa.
- Generar criterios de evaluación, de impacto y de aceptación del riesgo de cada activo.
- Definir los alcances y límites: garantizar que todos los activos se tomen en consideración, de acuerdo a su relevancia y jerarquización de importancia.
- Asignar funciones, responsabilidades y establecer una ruta para escalar decisiones y especificar los registros que se deben conservar respecto a la vulnerabilidad de cada activo.

- Valoración del riesgo, identificación y descripción cuantitativa y cualitativa del riesgo, lo que permite priorizar frente a los criterios de evaluación del riesgo establecidos para la organización.

- Identificación del riesgo, permite inferir por una pérdida potencial y como y donde podría generarse esta pérdida.

- Identificación de los activos: relaciona la cantidad de activos y su relevancia, así como el propietario o responsable del mismo.

- Identificación de las vulnerabilidades: buscar información sobre las vulnerabilidades y sus orígenes. Generar una línea de tiempo de exposición al riesgo y a sus transformaciones tecnológicas.

Video

Antes de continuar los invito a ver la video cápsula "Vulnerabilidades en la informática", la cual explica los principales tipos de vulnerabilidades que afectan la información.

"Vulnerabilidades en la Informática"

https://www.youtube.com/watch?v=i3CTOvutACc

Estudio de caso

Analicemos el siguiente caso de vulnerabilidad en una red:

Una microempresa cuenta con 7 computadores conectados a internet, con la configuración por defecto de fábrica, cada uno de ellos tiene configurada una cuenta de correo electrónico pública, por la cual recibe mensajería electrónica a diario, además, cuenta con software antivirus, instalado cuando compró los equipos hace más de un año y no se ha actualizado desde entonces, por otra parte tienen instalado un software de ofimática no licenciado y algunos colaboradores han instalado, reproductores de música, editores de video y otros software desde internet.

Antivirus
Programas destinados a detectar malware en los dispositivos.

USB
Puerto serial universal

¿A qué vulnerabilidades está expuesta esta red?

Antes de iniciar con el análisis es importante aclarar que, aunque existan vulnerabilidades en el sistema y/o red, esto no significa que se produzca un daño en forma automática, es decir, la red y los equipos tienen puntos débiles susceptibles a ser vulnerados, no por eso va a presentar fallas o deficiencias, pero si se expone en un alto porcentaje a que sea afectado por un ataque a esos puntos débiles.

Para el ejemplo desarrollaremos un análisis de vulnerabilidades global no detallado.

1. El primer dato importante que obtenemos, es que los equipos están configurados por defecto de fábrica, esto quiere decir que no tiene habilitada ninguna política de seguridad, con esto me refiero a:

   - No existe control de usuarios y contraseñas (políticas de acceso).
   - Ausencia del control de la información, ya que los puertos USB están habilitados, las unidades de DVD/CD están activas, permitiendo que cualquier usuario que tenga acceso a dichos equipos extraiga la información valiosa e importante para la empresa.
   - No se cuenta con políticas de usuario permitiendo que los colaboradores instalen cualquier tipo de software sin control.

Estudio de caso

2. Otro dato importante es que los equipos salen libremente a internet, esto vulnera la red pues no existe control de navegación web, permitiendo y/o facilitando que malwares en la nube accedan a la red, además, afectará el rendimiento de la misma, pues es probable que los usuarios con libre acceso permanezcan conectados a redes sociales y/o a páginas de videos (YouTube, Vimeo), consumiéndose los recursos de la red y ralentizando el servicio de la misma.

3. Correos electrónicos públicos no institucionales, esta es otra vulnerabilidad que presenta la red, ya que, al ser públicos no institucionales, no hay control ni seguimiento a la información que comparten los usuarios por estos medios, ni control de descargas de archivos adjuntos, haciéndola vulnerable al espionaje, robo de información o acceso abusivo a los datos, pues permite que los usuarios compartan información sensible de la empresa. Además, hace la red vulnerable a virus, troyanos, y demás tipos de malwares.

4. Otra vulnerabilidad es que cuenta con antivirus, pero este no está actualizado, la fortaleza de los antivirus radica en sus actualizaciones ya que a diario salen nuevos malwares y virus, si esta herramienta no está actualizada no prestan un servicio óptimo.

Malwares
Se refiere a programas maliciosos

Ralentizar
Hace referencia a colocar lenta la red o el sistema informático.

5. El software no legal además de ser un delito, es otra gran vulnerabilidad pues genera huecos de seguridad que permiten a los delincuentes acceder de forma abusiva a los equipos de cómputo de la compañía con diversos fines. Además de no permitir actualizar las fallas de seguridad que los fabricantes del software encuentran y corrigen, lo que se conoce como parches de seguridad o services pack, en el caso de Windows son programas que incluyen mejoras de seguridad, rendimiento y compatibilidad.

Estudio de caso

6. Por último, permitir que los usuarios instalen software ya sea desde dispositivos extraíbles o desde internet genera una vulnerabilidad a la red, el software no está autorizado por la compañía, y la instalación del mismo no viene garantiza, los certificados de validez no están activos o las firmas digitales han sido vulneradas, con el objetivo de agregar malware a dicho programa. La política de la compañía debe hacer énfasis en que sólo el departamento de TI se encargue de instalar el software requerido.

Con este ejercicio se pretende generar conciencia de la importancia de desarrollar políticas de seguridad tendientes a mejorar la disponibilidad, confidencialidad e integridad de la información tanto en las compañías como en el hogar.

Se ha dado una visión somera de las vulnerabilidades, pero podríamos comenzar a detallar cada una de estas y otras más que no se han nombrado, en cursos posteriores de seguridad se ahondará en este tema.

Lectura recomendada

Para reafirmar los conocimientos adquiridos hasta el momento los invito a realizar la siguiente lectura, la cual describe las principales amenazas y vulnerabilidades a las que están expuestos los sistemas informáticos y genera recomendaciones para minimizar los riesgos.

Guía de implementación de Seguridad de la información en una MIPYME.

Ministerio de Tecnologías de la Información y las Comunicaciones

Instrucción

Con el fin de una mejor apropiación de los aprendizajes, le invitamos a realizar la actividad caso simulado que se encuentra en la página principal del eje.

Seguridad en redes inalámbricas

En esta sección desarrollaremos un ejercicio práctico con la ayuda del simulador *Packet Tracer,* en el cual se implementará el control de acceso y la seguridad en una red Wi-Fi, subsanando algunas vulnerabilidades que presentan los dispositivos cuando se dejan configurados por defecto.

Las redes Wi-Fi referenciadas con el estándar IEEE802.11/b/g/n según sus características, presentan varias vulnerabilidades que pueden subsanarse de forma muy simple reduciendo el riesgo de la red y de la información que viaja por ella.

Para empezar, observemos las características fundamentales del estándar IEEE802.11:

Estándar	Características
IEEE802.11b	• Velocidad de transmisión 11 Mbps. • Frecuencia 2.4Ghz.
IEEE802.11g	• Velocidad de transmisión 54 Mbps. • Frecuencia 2.4Ghz.
IEEE802.11n	• Velocidad de transmisión hasta 600 Mbps, en la actualidad los dispositivos trabajan a velocidades de 150Mbs y 300Mbps. • Frecuencia 2.4Ghz y 5Ghz.

Tabla 2. Características estándar IEEE802.11
Fuente: IEEE802.11

Los router Wi-Fi o dispositivos multipropósito son los dispositivos de mayor uso en los hogares y las empresas, por cumplir varias funciones (router, switch, AP) y su bajo costo, pero así mismo su configuración inicial presenta varias vulnerabilidades.

Observa la imagen ¿has visto algún dispositivo parecido?

Figura 4 Router Wi-Fi
Fuente: freepik.com/4122

Video

Para una mejor comprensión del tema, los invito a ver el video relato "Control de acceso y seguridad en redes inalámbricas" en el cual explico la forma de subsanar algunas vulnerabilidades que traen los dispositivos router Wi-Fi en su configuración por defecto.

Video Relato CONTROL DE ACCESO

https://vimeo.com/244855348

De igual forma y a modo de síntesis observemos el siguiente mapa de vulnerabilidades.

Figura 5. Gestión de vulnerabilidades
Fuente: propia

Instrucción

En este punto, desarrolle los retos que encontrará en la página principal del eje

Lectura recomendada

Como complemento al eje 3 los invito a desarrollar la siguiente lectura, con la cual reafirmará los conocimientos adquiridos respecto a la seguridad y vulnerabilidades.

Seguridad en redes inalámbricas.

Panda software International, S.L.

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.