PASOS PARA OBTENER SEGURIDAD TRATANDO LAS VULNERABILIDADES; Y CÓMO REALIZAR UN SEGUIMIENTO EFECTIVO A LA SOLUCIÓN DE LAS VULNERABILIDADES TECNOLÓGICAS

William Rene Alvarado Ordoñez
weao33@hotmail.com
Universidad Piloto de Colombia

Resumen – Este artículo surge como una propuesta a partir de los conocimientos académicos adquiridos en las prácticas de seguridad realizadas en el desarrollo del seminario de investigación aplicada (SIA), de igual manera encuentra fundamento teórico, en la reflexión motivada desde las discusiones los diferentes módulos en dónde se profundizaron conceptos fundamentales para la seguridad y vulnerabilidad tecnológica

Sustentado en lo anterior, se decide establecer una serie de pasos que permiten complementar las pruebas de vulnerabilidad, la identificación de amenazas y el seguimiento efectivo, así como la identificación de algunas herramientas que apoyan lo mencionado, muestra de indicadores de gestión, los cuales son importantes para ver cómo está el estado de la empresa en seguridad y de las gestión de remediación.

Es pertinente mencionar entonces, que en los lineamientos de seguridad, las nuevas tecnologías de comunicaciones plantean la necesidad de mantener la confidencialidad; para ello, es especialmente importante diseñar e implantar sistemas y métodos de seguridad como los estudiados ampliamente en el seminario señalado anteriormente, en donde la identificación de vulnerabilidades, y exponer las mejores prácticas, de diseño y configuración para proporcionar un nivel de ingeniería de red y de seguridad de la información a una infraestructura y proteger las tecnologías y sistemas ante eventuales amenazas. A esto se añade que el núcleo del negocio no debe parar; dado que es la capacitación especializada, la que conforma profesionales especializados en seguridad para que identifiquen, implementen y gestionen de manera eficaz y segura un sistema de información.

Aceptado lo anterior, lo que se pretende en este artículo, es conocer y mejorar las variables importantes de un sistema como son la confidencialidad, integridad y disponibilidad, acorde a las mejores prácticas de manera tal que se realice la gestión de vulnerabilidades acorde a los lineamientos establecidos en la norma ISO 27001-2013 y al conocimiento adquirido en toda la especialización y el seminario SIA. Por tanto, en los pasos se establecerán recomendaciones para evidenciar las fallas tecnológicas desde el punto de vista de vulnerabilidades, se describirá a su vez, el proceso completo relacionado a un tratamiento de vulnerabilidades tecnológicas, y que suelen estar asociados a temas tan importantes como el análisis de riesgos.

Palabras clave: Seguridad, tecnología, riesgo informático, herramientas, red e información.

Abstract - This article comes as a proposal from the academic knowledge acquired in safety practices conducted in the seminar of applied research (SIA), likewise is theoretical foundation, reflection motivated from the discussions the different modules where fundamental concepts for security and technological vulnerability deepened.

Supported on the above, it decided to establish a series of steps that complement vulnerability testing, identifying threats and effective monitoring and identifying some tools that support the above, sample management indicators , which are important to see how the state enterprise security management and remediation.

It is pertinent to mention then, that safety guidelines , new communications technologies pose the need to maintain confidentiality; for it is especially important to design and implement systems and security methods as widely studied in the seminar noted above, where the identification of vulnerabilities and expose best practices, design and configuration to provide a level of network engineering and security of information infrastructure and protect technologies and systems against possible threats. To this is added to the core business should not stop; since it is the specialized training, forming specialized security professionals to identify, implement and manage effective and safe information system.

Accepted the above, what is intended in this article, it is to understand and improve the important variables of a system such as confidentiality, integrity and availability, according to the best practices so that vulnerability management is carried out according to the guidelines established in ISO 27001-2013 standard and knowledge acquired throughout specialization and SIA seminar. Therefore, in steps recommendations will be established to demonstrate the technological failures from the point of view of vulnerabilities, will be described in turn, the entire process related to treatment of technological vulnerabilities, and that are often associated with important issues such as the risk analysis.

Keywords: Safety, technology, computer risk, hardware, network and information.

I. INTRODUCCIÓN

Las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y así concretarlas en documentos que orienten las acciones de las mismas, permitiendo así mejorar los niveles de seguridad y reduciendo los riesgos tecnológicos que puedan llegar a afectar a la empresa.

Los ingenieros de seguridad pueden apoyar a la empresa en definir políticas y lineamientos de seguridad permitiendo con esto mejorar los controles asociados a las tecnologías, minimizando los riesgos tecnológicos y las tendencias de ataques como los del día cero, con la identificación de las vulnerabilidades técnicas, y proponer soluciones asociadas a un plan de remediación.

Por otra parte, realizar un seguimiento claro y detallado a las vulnerabilidades encontradas en todos los dispositivos, y orientar a la posible solución tecnológica ayuda a tener un conocimiento de sus riesgos identificados, debido a que la documentación es muy importante se recomienda realizar toda la documentación que permite tener continuidad de los trabajos realizados, y establecer como es el estado actual de las vulnerabilidades detectadas, éstas

recomendaciones apoyarán a las políticas generales de seguridad, facilitando la obtención de un adecuado nivel de control en la seguridad de la información, lo cual permite evitar y/o disminuir las fallas de seguridad en los equipos informáticos, sistemas, redes; reduciendo la posibilidad de que los ataques informáticos sean exitosos y reduciendo los posibles desastres, antes que estos, se materialicen o sean aprovechados por personas externas.

Los resultados e informes que apoyan la identificación de vulnerabilidades pueden ser los siguientes:

- ✓ Informes de los escaneos realizados a los dispositivos tecnológicos, con las vulnerabilidades encontradas y las posibles soluciones planteadas.
- ✓ Plan de solución propuesto para ejecutar la remediación en los diferentes servicios tecnológicos evaluados.
- ✓ Indicadores de seguimiento de remediación.
- ✓ Documentación de las vulnerabilidades encontradas y su estado.

II. CARACTERÍSTICAS

La seguridad de la información debe establecer las políticas o normas que permitan llevar los riesgos a un nivel aceptable por la compañía. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad; estas recomendaciones permiten mejorar la madurez del sistema de seguridad, minimizando el impacto de los trabajadores con respecto a los trabajos adicionales por temas de seguridad no establecidos en general.

Para la mayoría de los expertos en seguridad, el concepto de esta, es sólo un supuesto, porque no existe un sistema 100% seguro. Por tanto para que un sistema se pueda definir como seguro debe tener estas cuatro características: tres de esas características están referenciadas en la norma ISO 27001-2013.

Integridad: Cualidad de la información que se considera exacta, completa, homogénea, sólida y coherente con la intención de los creadores de esos datos. Esta cualidad, se obtiene cuando se impide eficazmente la inserción, modificación o destrucción no autorizada, sea accidental o intencional del contenido de una base de datos.

Confidencialidad: Se trata de una propiedad de la información que pretende garantizar el acceso sólo a las personas autorizadas.

Disponibilidad: El sistema se mantiene funcionando eficientemente y es capaz de recuperarse rápidamente en caso de fallo.

No repudio: El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

De esta forma, dependiendo de las fuentes de amenaza la seguridad puede dividirse en tres partes: seguridad física, seguridad ambiental y seguridad lógica.

La seguridad está orientada en proteger los activos informáticos, entre los que se encuentran los siguientes:

- ✓ La infraestructura computacional: Es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es

aplicar los controles, que los equipos funcionen adecuadamente, que tengan todos los sistemas de auditorías establecidos con el fin de poder anticiparse en caso de fallas, robos, y cualquier otro factor que atente contra la infraestructura informática.

- ✓ Los usuarios: Son las personas que utilizan la estructura tecnológica, comunicaciones y que gestionan la información. Los sistemas deben protegerse para que el uso por parte de ellos sea efectivo y seguro, sumado a ello, la seguridad de la información ayuda a que la información que manejan o almacenan no sea vulnerable.
- ✓ La información: Es el principal activo y es utilizada por los usuarios.

Es por tanto, que los riesgos a los que una compañía se pueden enfrentar se definen como, aquella eventualidad que imposibilita el cumplimiento de un objetivo, y según la Organización Internacional por la Normalización (ISO) versión 27001-2013 define riesgo tecnológico como "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños"; de tal forma la evaluación de estos riesgos identifica las amenazas, sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Existen dos puntos importantes a considerar son:

- ✓ La probabilidad de una amenaza.
- ✓ La magnitud del impacto sobre el sistema, la cual se mide por el nivel de degradación de uno o combinación de alguno de los elementos, como confidencialidad, disponibilidad, integridad.

a. Determinar la probabilidad

Con el fin de evaluar una probabilidad o una estimación de la ocurrencia de un evento, los siguientes factores deben ser tomados en cuenta:

- ✓ Fuente de la amenaza y su capacidad.
- ✓ Naturaleza de la vulnerabilidad.

La probabilidad que una vulnerabilidad potencial pueda ser explotada por una fuente de amenaza la podemos clasificar en alta, media-alta, media, media- baja y baja, como se describe a continuación:

Figura 1 Probabilidad de ocurrencia de un evento.

Nivel	Definición
Alta = 5	La amenaza está altamente motivada y es suficientemente capaz de llevarse a cabo
Media Alta = 4	La amenaza está fundamentada y es posible.
Media = 3	La amenaza no es posible
Media Baja = 2	La amenaza no posee la suficiente capacidad.
Baja = 1	La amenaza no posee la suficiente motivación y capacidad.

Fuente: Autor

En la figura 1, se quiere mostrar las posibilidades clasificadas en 4 niveles que hay que contemplar frente a una amenaza.

b. Activos críticos

Un inventario actualizado y completo de los activos, es un prerrequisito para una gestión eficaz de la vulnerabilidad técnica. La información específica necesaria para apoyar la gestión de la vulnerabilidad técnica incluye: al vendedor del software, los números de las versiones, el estado actual de despliegue (por ejemplo, qué software se

instaló en qué sistema), y la(s) persona(s) dentro de la organización responsable por el software, también hacen parte de los activos hardware, software y bases de datos.

Los activos pueden o no, ser propiedad de la empresa, pero cualquier equipo o información bajo el control de la organización o que se integre en la operación debe ser considerado para su inclusión en el análisis. Esto incluye, los sistemas informáticos operados en los sitios de los proveedores, incluso terceros que pueden contener información confidencial, y pueden ser utilizados para causar daño si se conecta a red.

Los sistemas informáticos que deben tenerse en cuenta, son los que se utilizan para control de procesos, operación de sistemas de seguridad, operación de servicios, las comunicaciones, acceso a las instalaciones, almacenamiento de información y redes.

Entre los lugares que necesitan ser protegidos se incluyen salas de ordenadores, salas de servidores, salas de control de procesos y estaciones, salas de rack.

Hay una pregunta clave que deben ser abordada para determinar si los activos de la organización son vulnerables:

¿Tienen los atributos que permiten su uso para causar daño a la organización?

Los activos no tienen por qué ser intrínsecamente vulnerables para que puedan ser utilizados para causar daño a la organización. Es a través de la manipulación, robo / daño de la información de los sistemas informáticos que sufren daños y que afectan una organización. Atributos de los sistemas informáticos que incluyen su valor financiero, los datos almacenados y la información, y el potencial para la manipulación o el apagado. Los atributos de información incluyen el valor para el competidor, el costo de reproducirla, y la utilidad para un asaltante. Y el atributo clave para las personas es el valor inherente de la vida humana.

III. OBJETIVO DEL ANÁLISIS DE VULNERABILIDADES

El objetivo de análisis de vulnerabilidades, se utiliza para identificar las amenazas y deficiencias tecnológicas y posibles objetivos en las instalaciones de la organización.

El objetivo del análisis implica:

- ✓ La identificación de la probabilidad, que la organización puede ser objetivo de ataque por culpa de las fallas tecnológicas no detectadas a tiempo.
- ✓ La identificación de los activos críticos dentro de las instalaciones que pueden ser atacados.

IV. ANÁLISIS DE AMENAZAS

Las amenazas requieren que un atacante esté motivado con la intención de causar daño. Además los atacantes son capaces y más si tienen la posibilidad de acceder a un activo y lo utilizan para lograr sus objetivos. El análisis de amenazas implica la identificación del origen y tipos de amenazas creíbles y opcionalmente, su criticidad.

Estas amenazas pueden surgir desde el exterior (por ejemplo, terroristas, saboteadores, criminales, hackers, activistas, etc.), internamente de las personas que tienen alguna medida de un acceso sin restricciones a una instalación (por ejemplo, empleados inconformes, contratistas, clientes, proveedores u otros), o de unión entre propios y extraños. Las amenazas pueden ser de personas o grupos.

También hay que identificar los tipos de amenazas, es decir, decidir conocer los

objetivos o intenciones de los adversarios potenciales.

Por otro lado, si existen los adversarios, éstos pueden querer causar daño a los empleados, el público, una institución, una industria, la economía, la seguridad nacional, etc. En concreto, las siguientes amenazas cibernéticas deben ser consideradas:

- ✓ Incapacidad: daño o destrucción de recursos tecnológicos con el fin de causar una pérdida financiera, por ejemplo, ataque físico, corte de cables, negación de servicio.
- ✓ La pérdida: robo, divulgación, daño, destrucción o corrupción de los datos o la información almacenada en los activos tecnológicos, por ejemplo, la piratería, el robo de medios de almacenamiento, comunicaciones y computadores.

A veces el análisis de amenazas incluye la estimación de la criticidad (probabilidad y gravedad) de las amenazas específicas a fin de priorizar o seleccionarlas para el análisis de vulnerabilidades.

Los factores que deben tenerse en cuenta en la estimación de la probabilidad de amenazas específicas: incluyen la motivación, las capacidades, intenciones, características y tácticas de atacantes.

Las principales amenazas, se pueden identificar mediante la revisión de listas de control de agresores potenciales y teniendo en cuenta la información disponible sobre las amenazas actuales.

Las amenazas, se combinan con los activos para identificar eventos de amenaza, o maneras de como los activos pueden ser explotados o comprometidos; es decir, se utilizan de alguna manera para causar daño.

Son estos emparejamientos que se estudian en el análisis de vulnerabilidad.

V. RECOMENDADAS PARA LA IDENTIFICACIÓN, Y GESTIÓN DE VULNERABILIDADES Y EL SEGUIMIENTO EFECTIVO.

La seguridad, se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad, de acuerdo con la Norma ISO 27001-2013.

Basados en estos tres principios de seguridad, se realizó unas recomendaciones de seguridad de vulnerabilidades, el cual tiene una serie de componentes que deben conocerse con el fin de identificar los riesgos tecnológicos que integrados a una metodología de análisis permite identificar los “huecos” de seguridad, con unos riesgos puntuales que dependiendo del apetito de estos riesgos se tendrán o no en un plan de acción, y será de gran ayuda para fortalecer la seguridad tecnológica.

Es importante que para la seguridad se deban tener muy claros los siguientes criterios, i) conocer el peligro, ii) clasificarlo y iii) protegerse de los impactos o daños de la mejor manera posible. Esto significa, que solamente cuando se está consciente de las potenciales amenazas, agresores y sus intenciones dañinas (directas o indirectas) en contra de la compañía, se pueden tomar medidas de protección adecuadas, para que no se pierda o dañen recursos valiosos.

En este sentido, la seguridad sirve para la protección de la información, en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella.

a) Estrategia de pruebas

Con la estrategia de pruebas, lo que se busca es dar a conocer algunos de los pasos que se realizan para ejecutar las pruebas de seguridad, estos pasos son importantes porque permiten realizar una preparación previa para realizar las pruebas de vulnerabilidad y que permiten ayudar a obtener información tecnológica de los dispositivos como de las pruebas realizadas, estos pasos son ejecutados con las diferentes herramientas instaladas, los conocimientos del personal de apoyo como el consultor de seguridad y también la participación en algunos casos de los administradores de las diferentes plataformas tecnológicas.

Mientras que, para el desarrollo de las pruebas de búsqueda de vulnerabilidades se aborda un enfoque de tipo caja blanca, hay que recordar que el enfoque caja blanca es donde se tiene alguna información tecnológica como por ejemplo dirección IP, la dirección Mac o el nombre de la máquina, del dispositivo sobre el cual se ejecutan las pruebas.

- ✓ **Test de verificación**: Consiste en realizar un sondeo rápido por medio de las herramientas instaladas, para este caso casi siempre se utiliza la herramienta Netscan y Nmap, para ver si hay acceso a los dispositivos tecnológicos a evaluar.
- ✓ **Sondeo de red**: Recolectar información básica acerca de los objetivos a evaluar, como IP y si el dispositivo tiene visibilidad por parte de la herramienta de seguridad con la que se realiza el sondeo.
- ✓ Identificación de servicios: Enumerar servicios de internet activo o accesible.
- ✓ Búsqueda y verificación de vulnerabilidades: Identificar, comprender y verificar las debilidades, errores de configuración y vulnerabilidades en el servidor.
- ✓ Lógica y controles: Depurar falsos positivos realizando ajustes en las herramientas de análisis para verificar los resultados y entregarlos ajustados

Las actividades desarrolladas durante el proceso de pruebas son:

***Reconocimiento y Escáner de puertos:**

- ✓ Exploración
- ✓ Descubrimiento de equipos
- ✓ Detección de conexiones externas
- ✓ Obtención de rangos de direcciones IP
- ✓ Detección de puertos (TCP, UDP, etc.)
- ✓ Detección de servicios
- ✓ Sniffing de red

****Definición de pruebas y herramientas a utilizar:**

- ✓ Como parte de la metodología de trabajo, el inventario de pruebas y herramientas necesarias para la ejecución de las mismas, se definen con base en la información obtenida durante las actividades de reconocimiento.

*****Desarrollo de las pruebas:**

- ✓ Pruebas de búsqueda de Vulnerabilidades
- ✓ Pruebas de explotación de Vulnerabilidades.

b) Herramientas de seguridad

En las recomendaciones de seguridad se sugiere utilizar una serie de componentes tecnológicos los cuales hacen parte importante,

uno de estos componentes es el (appliance), el cual es una herramienta con un hardware específico, tipo servidor en el cual estará la aplicación de escaneo de vulnerabilidades y otras herramientas de seguridad.

En las recomendaciones de seguridad, se decide contar con una serie de herramientas especializadas como Kali Linux, Acunetix, Nmap, Foca, Linux, Netscan Nessus, Port Scan entre otras, que permiten apoyar, las verificaciones y complementar los informes de las herramientas del mercado, estas también permiten detectar las vulnerabilidades y los riesgos tecnológicos asociados a las debilidades, esto debido a que con una sola herramienta no es posible cubrir todas las recomendación.

Estas herramientas, son instaladas previamente en un servidor con diferentes máquinas virtuales las cuales permiten realizar la instalación fácilmente, sin generar conflictos o lentitudes en los servicios, se toma la decisión de proponer un servidor debido a que si son escaneos a un número importante de direcciones IP, necesitará que la herramienta cuente con los recursos necesarios para que el aplicativo funcione sin problema, para cumplir con el numeral 7 de la circular reglamentaria de Súper Intendencia de Financiera, para entidades financieras la cual menciona que para las pruebas de vulnerabilidad se deben tener un equipo completamente independiente y dedicado para este servicio.

Tabla 1 Cuadro de herramientas de seguridad

HERRAMIENTAS UTILIZADAS	
	Nmap ("Network Mapper") es una herramienta libre y de código abierto muy útil en ejecución de auditorías de seguridad. Usa paquetes IP de forma novedosa para determinar qué hosts están disponibles, qué servicios están ejecutando, qué sistemas operativos están corriendo, qué tipo de filtrado de paquetes está en uso, entre otras características. Se ejecuta Linux, Windows y Mac OS X. Incluye una interfaz gráfica (Zenmap), una herramienta de depuración (Ncat), una utilidad para comparación de resultados (Ndiff), y una herramienta de generación de paquetes y análisis de respuesta (Nping). http://nmap.org/
	KALI LINUX es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad. Kali es una completa re-construcción de BackTrack Linux desde la base hacia arriba, y se adhiere completamente a los estándares de desarrollo de Debian. http://www.kali.org/
	**METASPLOIT FRAMEWORK** es un conjunto de herramientas con las que se pueden desarrollar y ejecutar exploits contra maquinas remotas para comprobar la seguridad de estas. Otras de las funcionalidades que aporta es un archivo de shellcodes, herramientas para recolectar información y escanear en busca de vulnerabilidades. El extensible modelo a través del cual los payloads, encoders, no-op generators y exploits pueden integrarse ha hecho posible el uso de Metasploit Framework como una salida para la investigación de la explotación de vanguardia. http://www.rapid7.com/products/metasploit/
	XSS es la abreviatura de Cross-SiteScriping, una manera de atacar los sitios a través de vulnerabilidades XSS en la inyección de códigos HTML. La herramienta busca los puntos de entrada posibles para ataques contra el sistema. Los ataques XSS pueden causar graves daños a las aplicaciones web. En definitiva, XSS Me te ayuda a detectar las vulnerabilidades XSS para proteger tus aplicaciones de errores innecesarios.
	Sqlmap es una herramienta de pruebas de penetración de código abierto, que automatiza el proceso de detectar y explotar los errores de inyección SQL y hacerse cargo de los servidores de bases de datos. Viene con un potente motor de detección, muchas características de nicho para el probador de la penetración final y una amplia gama de interruptores con una duración de toma de huellas dactilares de base de datos, a lo largo de captación de datos de la base de datos, para acceder al sistema de archivos subyacente y ejecutar comandos en el sistema operativo a través de fuera conexiones de banda. http://sqlmap.org/
	Acunetix es un escáner de vulnerabilidades de aplicaciones web. La herramienta está diseñada para encontrar agujeros de seguridad en la aplicación web de la organización que un atacante podría aprovechar para obtener acceso a los sistemas y datos.
Vega	Vega es un escáner de código y pruebas de plataforma libre y abierta para probar la seguridad de las aplicaciones web. Vega puede ayudarle a encontrar y validar la inyección de SQL, Cross-Site Scripting (XSS), inadvertidamente revelado información sensible, y otras vulnerabilidades. Está escrito en Java, GUI basada, y se ejecuta en Linux, OS X y Windows.

Fuente: Autor

En la Tabla 1, se muestra algunas de las herramientas que se utilizan en las recomendaciones de seguridad, con las descripciones de la herramienta y el servicio que realiza.

c) Análisis de vulnerabilidades

Por medio del análisis de vulnerabilidades, lo que se busca es poder identificar los huecos o malas prácticas de seguridad, y las amenazas, así se podrán corregir las deficiencias antes de que sean explotadas, estas pueden ser identificadas en cualquier infraestructura tecnológica, la identificación de las vulnerabilidad se hace por medio de una herramienta especializada como por ejemplo (Aplicación SOX (AVOCET, Symantec, FAV, SAINT o cualquiera que esté en el mercado), estas herramientas realizan un sondeo a los dispositivo tecnológicos los cuales son registrados en la herramienta por la dirección IP, este sondeo es programado dentro de una ventana de mantenimiento acordada, una vez terminado el sondeo se ejecuta el informe.

Figura 2 Informe de identificación de vulnerabilidades Herramienta Saint

Host Name	Port	Vulnerability / service	Class	CVE	CVSS
Equipo 1		H323 Service May be vulnerable to buffer overflow	Networking SNMP	2003-0819 2004-0054 2004-0056	10
Equipo 2	1720 /TCP	TCP Timestamp request enable	Other		2
Equipo 3	1720 /TCP	h323 hostcall			

Fuente: Autor

Por otra parte en la Figura 2, permite identificar el Host Name, el cual hace referencia a la dirección IP del equipo escaneado, por su parte la columna Port, hace referencia al puerto afectado del equipos escaneado, seguidamente en la Columna Vulnerability / Service, se observa el servicio al cual está asociado la vulnerabilidad, a su lado, la columna Class, se hace referencia a qué tipo de tecnología, para este caso es Networking, a su vez la Columna CVE (Common vulnerabilities and exposure) hace referencia a la vulnerabilidad detectada, para este informe fueron las vulnerabilidades asociadas a los números 2003-0818, 2004-0054 y 2004-0056, finalmente esta la columna CVSS (Common vulnerability scoring system), en la cual se ve la calificación de las vulnerabilidades detectadas.

Como se muestra en la figura, se puede observar la identificación de las vulnerabilidades.

d) Propuesta de Controles para el Fortalecimiento Tecnológico

Se hace indispensable, dar a conocer qué tipos de controles y recomendaciones son las apropiadas para fortalecer las tecnologías de la empresa, tomando como base lo señalado anteriormente, la propuesta de seguridad establece sugerir controles para el fortalecimiento tecnológico, que permitan contribuir con la solución de las vulnerabilidades, los controles pueden ser, aplicación de parches, guías de aseguramiento, segmentación de red, cierre de puertos activos, desactivar protocolos inseguros, eliminar puertas traseras, desactivar servicios que no se necesiten, eliminación de cuentas de usuarios con privilegios elevados, eliminar carpetas compartidas, eliminar usuarios y password por defecto, entre otras, esto ayuda remediar las debilidades identificadas, en la propuesta de seguridad, el personal técnico de la empresa se puede apoyar con los especialistas propuestos para dicha labor, que es el consultor

de seguridad. Lo anterior se puede verificar en la figura que se presenta a continuación.

Figura 3 Informe de controles técnicos propuestos

CONTROL PROPUESTO	**Actualiza Application Express a por lo menos la versión 3.2.1. (Última versión estable "4.2.2") Enlace de descarga: http://www.oracle.com/technetwork/developer-tools/apex/overview/index.html**
MAS INFORMACIÓN	http://www.oracle.com/technetwork/developer-tools/apex/index.html http://www.oracle.com/technetwork/topics/security/cpujul2010-155308.html http://www.nessus.org/u?3955a3de
CONTROL PROPUESTO	Actualiza Application Express a por lo menos la versión 4.1. (Ultima versión estable "4.2.2") Enlace de descarga: http://www.oracle.com/technetwork/developer-tools/apex/overview/index.html
MAS INFORMACIÓN	http://www.oracle.com/technetwork/developer-tools/apex/index.html http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html http://www.recx.co.uk/research/index.php?item=CVE-2011-3525
CONTROL PROPUESTO	Desactivar estos métodos.
MAS INFORMACIÓN	http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf http://www.apacheweek.com/issues/03-01-24 http://download.oracle.com/sunalerts/1000718.1.html
CONTROL PROPUESTO	Comprar o generar un certificado adecuado para este servicio.
MAS INFORMACIÓN	
CONTROL PROPUESTO	Obtenga un nuevo certificado firmado por una CA de confianza, tales como Thawte o VeriSign. Las instrucciones precisas para la obtención de un nuevo certificado dependen de las necesidades de su organización. Por lo general, usted tendrá que generar una solicitud de certificado y guardar la solicitud en un archivo. Este archivo se envía a una autoridad de certificación (CA) para su procesamiento. Después de tener recibido un nuevo archivo de certificado de la entidad emisora de certificados, tendrá que instalarlo en el servidor TLS / SSL.
MAS INFORMACIÓN	http://www.scip.ch/en/?nasldb.51192 http://www.accv.es/fileadmin/Archivos/Politicas_pdf/ACCV-CP-03V3.0-c.pdf https://www.digicert.com/es/instalar-certificado-ssl.htm https://www.digicert.com/es/instalar-certificado-ssl-apache.htm https://www.verisign.es/support/ssl-certificates-support/index.html

Fuente: Autor

e) Documentación

Este servicio de documentación, se propone debido a que los trabajos de remediación y de identificación de vulnerabilidad deben quedar documentados, esto con el fin que si hay una ausencia de la persona que está realizando la labor, la persona entrante pueda rápidamente tener conocimiento de las actividades realizadas, adicionalmente es importante debido a que la empresa cuenta con una base de datos de conocimiento en la cual puede ser aprovechada para realizar consultas con respecto a la remediación, esta idea surge debido a que las empresas no tiene información de las vulnerabilidades y es de vital importancia el conocimiento de las mismas, también se recomendó debido a que en las propuestas de seguridad no se establece este punto.

En la documentación, se establece que todos los trabajos que se realicen en pro de la remediación sean registrados en una base de datos de conocimiento. Adicionalmente las vulnerabilidades que no se puedan remediar por que impactan el CORE del negocio, o los cambios tecnológicos son muy altos, deben estar reportadas. Las vulnerabilidades tecnológicas que no apliquen son llamadas falsas positivas y deben ser registradas en el formato de declaración de vulnerabilidades, y el tiempo máximo de la documentación debe ser de un año.

Como las vulnerabilidades están asociadas a riesgos tecnólogos, aquellas que no se puedan remediar, alguien debe asumir este riesgo en caso que se materialicen y debe quedar registrada en un formato de aceptación de riesgo; esta aceptación de riesgo no debe ser indefinida, debe ser por un tiempo prudencial aproximadamente de un año hasta que se pueda realizar la remediación.

Para el registro de vulnerabilidades se puede utilizar un formato en el cual se registran las vulnerabilidades y el estado en el cual se encuentra, si es asumida, remediada o falso positivos.

f) Indicadores de gestión

Los indicadores de gestión, son medidas utilizadas para determinar el éxito de un proyecto o una organización. Los indicadores de gestión suelen establecerse por los líderes del proyecto u organización, y son posteriormente utilizados continuamente a lo largo del ciclo de vida, para evaluar el desempeño y los resultados.

Por la razón anteriormente expuesta, es importante establecer unos indicadores de gestión enfocados a las vulnerabilidades encontradas y que tienen o no un exploit, esto permite definir un tiempo de remediación que está establecido y llevar estadísticas de indicadores de mejora continua, este tipo de indicadores no son generados por ninguna herramienta de seguridad y es uno de valores agregados, este informe es diferente a los demás mencionados anteriormente debido a que está enfocado a los exploit de las vulnerabilidades y no al hallazgo de la vulnerabilidad detectada.

Dentro del contexto general de las vulnerabilidades, la siguiente tabla explica la forma en que son clasificadas las vulnerabilidades.

Tabla 2 Clasificación vulnerabilidades

Explotabilidad Criticidad	Con Exploit	Sin Exploit	Tiempo de atención y asistencia
Critica	X		< 1 m
Critica		X	< 1 m
Alta	X		< 1 m
Alta		X	< 2 m
Media	X		< 3 m
Media		X	< 3 m
Baja	X		< 4 m
Baja		X	< 4 m

Fuente: Autor

En la tabla 2, que son autorías del autor, se muestra una recomendación sobre los tiempos que se definen para la posible la remediación.

Nivel de evaluación.

- ✓ Inaceptable: Cuando se supera el criterio de medición.
- ✓ Tolerable: Cuando se está en medio de un criterio de medición.
- ✓ Aceptable: cuando se está por debajo de un criterio de medición.

***Indicadores de medición.**

Se han definido dos (2) indicadores de medición:

Vulnerabilidades con EXPLOIT (VCE) = PKI (VCE). Son aquellas vulnerabilidades de cualquier nivel de criticidad que poseen un EXPLOIT, que les permite materializarlas de manera inmediata.

El indicador y su meta están expresados en la siguiente figura:

Figura 4 Vulnerabilidad con exploit

PKI(vce)=[Total de Vulnerabilidades Explotables encontradas / Total de Vulnerabilidades Encontradas]*100	Trimestral	P(v)>=10%	0%>p(v)<10%	0%

Fuente: Autor

En la figura 6 se evidencian algunos indicadores propuestos.

Este indicador refleja, la forma en que se evalúa la presencia de las vulnerabilidades con EXPLOIT (VCE) dentro de las plataformas:

- ✓ Inaceptable: Que existan vulnerabilidades con EXPLOIT por encima del 10%.
- ✓ Tolerable: Que existan vulnerabilidades con EXPLOIT entre el 0 y 10%.
- ✓ Aceptable: Que las vulnerabilidades con EXPLOIT sean iguales al 0%.

Vulnerabilidades sin EXPLOIT (VSE) = PKI (VSE). Son aquellas vulnerabilidades de cualquier nivel de criticidad que no poseen un EXPLOIT, que les permite materializarlas inmediatamente.

Figura 5 Vulnerabilidad sin exploit

PKI(vse)=[Total de Vulnerabilidades no Explotables encontradas / Total de Vulnerabilidades Encontradas]*100	Trimestral	P(v)>=50%	25%>=P(v)<50 %	0%>=P(v)<25%

Fuente: Autor

En la figura 6 se evidencian algunos indicadores propuestos.

Este indicador refleja la forma en que se evalúa la presencia de las vulnerabilidades sin EXPLOIT (VSE) dentro de las plataformas:

- ✓ Inaceptable: Que existan Vulnerabilidades sin EXPLOIT por encima del 50%
- ✓ Tolerable: Que existan Vulnerabilidades sin EXPLOIT entre el 25 y 50%
- ✓ Aceptable: Que las vulnerabilidades sin EXPLOIT estén por debajo del 25%

Índice de variabilidad de las vulnerabilidades: muestra la relación entre cantidad de componentes evaluados y el total de vulnerabilidades que permitirá en el tiempo poder determinar la efectividad de los procesos de remediación.

IVV=índice de variabilidad de vulnerabilidades.
TV = Total de vulnerabilidades identificadas en una prueba de seguridad
CM = Cantidad de máquinas o tecnologías evaluadas en una prueba de seguridad.

g) Identificación del riesgo

Las recomendaciones de seguridad tienen como objetivo específico, identificar y alertar los riesgos en la infraestructura así como las acciones y mejores prácticas que pueden implementarse para minimizar el riesgo.

Para esto, tenemos en cuenta que el riesgo es la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o las amenazas, por separado, no representan un peligro. Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre.

Sin embargo, los riesgos pueden reducirse o manejarse. Si somos cuidadosos en nuestra relación con el ambiente, y si estamos conscientes de nuestras debilidades y vulnerabilidades frente a las amenazas existentes, se pueden tomar medidas como la remediación de vulnerabilidades para asegurar que las amenazas no se conviertan en desastres.

Basándose en los conceptos definidos lo que se hace, es identificar los riesgos existentes tomando como referencia los informes de vulnerabilidad, los cuales permiten identificar cual es el riesgo puntual así como se muestra en el cuadro adjunto.

Tabla 3 Cuadro de Riesgo

RIESGO IDENTIFICADO	NIVEL	OBJETIVO
Posible afectación del servicio e integridad del servidor, debido a la vulnerabilidad en apuntadores Oracle Apex.	Medio	10.1.141.58
Posible interpretación de tráfico, debido a criptografía SSL, que usa algoritmos Hash MD5 la cual tiene debilidades conocidas	Medio	10.1.141.58
Posible interpretación de tráfico, debido a certificado SSL expirado o con nombre de hots invalido, SSL con llaves débiles en RSA.	Medio	10.1.141.58
Pérdida de información sensible, por inyección de consultas causando por el método TRACE/TRACK en HTTP.	Medio	10.1.141.58
Posible revelación de información sensible debido a la talla de la configuración de Cookies de Apache.	Medio	10.1.141.58
Posible pérdida de la confidencialidad, integridad y disponibilidad de la base de datos remotamente debido a la ausencia de cifrado de credenciales en Oracle.	Alto	SERVIDORES 10.1.141.95 10.1.141.229

Fuente: Autor

En la tabla 3, son establecidas y realizadas por el autor, se identifican los tipos de riesgos, y los equipos impactados por estas vulnerabilidades.

h) Aportes de las recomendaciones de Seguridad

Estos datos de seguridad de vulnerabilidades, se apoyan en los estándares y normas de la seguridad en la información; y su principal aporte es ser un facilitador en el seguimiento de las vulnerabilidades y de medir su posible impacto para cualquier tipo de organización.

La misma, se ha enfocado en el análisis de la problemática de seguridad en la información, permitiendo brindar las bases que puedan facilitar procesos orientados a mejorar la seguridad informática en las diferentes organizaciones.

La estructura propuesta de seguridad de vulnerabilidades, se basa sobre la implementación práctica y concreta relacionada con las actividades que permitan dar seguridad a las organizaciones, de acuerdo a sus propias necesidades, lineamientos y perspectivas, buscando.

A su vez, en la implementación de esta se debe tener conocimiento de las funciones, tareas, actividades relacionadas con cada una de las etapas, con el fin de estructurar de forma adecuada su seguridad.

Por lo tanto, con las recomendaciones de seguridad se apoya a la empresa en definir un procedimiento para hacer frente a una situación en la que se ha identificado una vulnerabilidad, pero no hay una contramedida adecuada. En esta situación, la organización debería evaluar los riesgos relacionados con la vulnerabilidad conocida.

VI. CONCLUSIONES

Los resultados de los análisis de riesgos y de pruebas de vulnerabilidad, tienen información sobre las debilidades y vulnerabilidades que posee la organización, la cual podemos utilizar como punto de partida para tomar las decisiones con relación a la seguridad de la información.

Estas recomendaciones de seguridad se pueden implementará en cualquier empresa y se adaptara a ésta, más no la empresa se adaptara a las recomendaciones.

El apoyo de remediación con un adecuado aseguramiento, no protegerá permanentemente a las empresas de las vulnerabilidades tecnológicas; se debe realizar una actualización de controles periódicos, donde se pruebe el nivel de seguridad de los dispositivos, con el fin de proteger la información o los equipos de la organización.

La implementación de seguridad de vulnerabilidades, tendrá controles de seguridad de la información en las organizaciones, según las probabilidades de riesgos de seguridad en sus entornos informáticos, relacionados con el tratamiento de la información.

La seguridad de vulnerabilidades, es aplicable perfectamente en organizaciones que carecen de herramientas que permitan mantener niveles tolerables de seguridad, en relación con las potenciales amenazas de los entornos informáticos.

RECOMENDACIONES

Una vez implementada, es importante realizar las actividades que permitirán tener actualizada logrando su objetivo principal de conocer los riesgos, estas son:

Generar una cultura a nivel organizacional, que permita mantenerse actualizado en temas de seguridad de la información, mediante la suscripción a grupos

de noticias, boletines informativos y listas de seguridad.

Se recomienda, utilizar los recursos disponibles en Internet para tener conocimiento de las últimas versiones de parches y sugerencias en seguridad.

Filtrar comandos y servicios remotos que no sean necesarios dentro de cada servidor.

Depurar las configuraciones por defecto

Desarrollar un plan de trabajo entre las directivas y el departamento de TI, que permita la inclusión y priorización de seguridad de vulnerabilidades, y con ello materializar el compromiso y los niveles de inversión que estén dispuestos a asumir respecto a la seguridad en la Información y el funcionamiento del modelo.

Definir un plan de capacitación, tanto de las pruebas de vulnerabilidad como del levantamiento de riegos de los procesos; esto para que la empresa quede con la autonomía de realizar este tipo de verificaciones y no depender de un tercero.

Realizar evaluaciones periódicas, de seguridad con el fin de mejorarlo y aplicarlo a las empresas que están en crecimiento.

Definir reuniones de seguimiento planificadas, para la retro-alimentación de seguridad de vulnerabilidades; de tal manera que se pueda analizar que lo definido fue acertado o no, para el mejoramiento tanto del negocio como de la seguridad en la Información.

Incentivar en todos los actores (usuarios, proveedores, clientes, etc.,) tanto el cumplimiento de seguridad de vulnerabilidades, como la colaboración para lograr su adecuado funcionamiento, asegurando la arquitectura de seguridad en la información y los procesos de la misma.

REFERENCIAS BIBLIOGRÁFICAS

[1] Burgos Salazar, Jorge. Propuesta para seguridad de la información en TIC. Disponible en internet: < http://ceur- ws.org/Vol-488/paper13.pdf>

[2] Garzón, Daniel Santiago. Metodología de análisis de vulnerabilidades para empresas de mediana y pequeña escala. Disponible en internet: < http://www.javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf>

[3] Gómez Vieites, Álvaro. Enciclopedia de la seguridad informática: vulnerabilidades de los sistemas informáticos. 2 ed. México D.F.: Alfaomega Grupo Editor, 2011. p.173.

[4] Mejía, Quijano Rubí Consuelo, Administración de Riesgos Un Enfoque Empresarial. Disponible en internet: < http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/Nota%20de%20clase%2016%20Mapa%20de%20Riesgos.pDf>

[5] Mifsud, Elvira. Introducción a la seguridad informática – Vulnerabilidades de un sistema informático. Disponible en internet:< http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la- seguridad-informatica?start=3>

[6] Nocella, Daniel. Claves para implantar un Propuesta de seguridad informática exitoso. Negocios & Management. Disponible en internet:<http://negociosymanagement.com.ar/?p=2285>

[7] Pérez García, Camilo. ¿En Colombia se investigan los delitos informáticos?– Colombia digital. Disponible en: < http://www.colombiadigital.net/entorno-digital/articulos-de- contexto/item/4810-en-

colombia-se-investigan-los-delitos-informaticos.html>
[8] Security Models and Architecture. Chapter Disponible en internet: < http://cdn.ttgtmedia.com/searchSecurity/downloads/29667C05.pdf>
[9] Segu.Info. Vulnerar para proteger. Seguridad de la información. Disponible en internet: < http://www.segu-info.com.ar/proteccion/vulnerar.htm>
[10] http://www.undernews.fr/malwares- virus-antivirus/carbanak-malware-un- braquage-n