UNIVERSIDAD Rafael Belloso Chacín
Revista Electrónica de Estudios Telemáticos
TÉLÉMATIQUE

Metodología de modelado de amenazas para entornos informáticos de empresas aseguradoras

Threat modeling methodology for IT environments of insurance companies

Ing. Pirela Molina, Juan José
ingjuanpirelamolina@outlook.com
ORCID: 0000-0002-4979-7191

RESUMEN

El objetivo de esta investigación la elaboración de una metodología de modelado de amenazas enfocado en organizaciones dentro del sector asegurador en Caracas, Venezuela. Para conseguir el objetivo de este artículo, se empleó revisión bibliográfica de diversas metodologías de modelado de amenazas para identificar su focalización y métodos de análisis con el propósito de generar el modelo planteado. Así mismo, se evaluó el modelo a través de la aplicación de cada una de sus fases sobre una empresa aseguradora, cuya sede central se ubica en caracas Venezuela. La identificación de los objetivos del negocio y el alcance técnico de sus procesos críticos de negocio se logró a través de entrevistas al personal de TI (Tecnologías de la información). Posteriormente, se analizaron cada uno de los elementos de TI que componen los procesos críticos para identificar las vulnerabilidades de ciberseguridad en cada uno de ellos. Seguidamente, se categorizaron las amenazas para finalmente generar diagramas conceptuales para los vectores de ataque identificados, de tal forma que la empresa visualice el proceso del ataque y como este impacta en sus procesos de negocios. La metodología planteada probó ser útil para complementar los procesos de análisis de riesgo, así mismo, por la naturaleza de las empresas aseguradoras en Latinoamérica, esta es flexible para ser aplicada en cualquier otra empresa de este rubro dentro de la región.

Palabras clave: Ciberseguridad, Tecnologías de la información, Redes de datos, modelado de amenazas.

ABSTRACT

The objective of this research is to develop a threat modeling methodology focused on organizations within the insurance sector in Caracas, Venezuela. To achieve the objective of this article, a bibliographic review of various threat modeling methodologies was used to identify their focus and analysis methods to generate the proposed model. Likewise, the model was evaluated through the application of each of its phases on an insurance company, whose headquarters are in Caracas, Venezuela. The identification of the business objectives and the technical scope of its critical business processes was achieved through interviews with IT (Information Technology) personnel. Subsequently, each of the IT elements that make up the critical processes were analyzed to identify the cybersecurity vulnerabilities in each of them. Next, the threats were categorized to finally generate conceptual diagrams for the identified attack vectors, so that the company can visualize the attack process and how it impacts its business processes. The proposed methodology proved to be useful to complement the risk analysis processes. Furthermore, due to the nature of insurance companies in Latin America, it is flexible to be applied to any other company in this sector within the region.

Keywords: Cybersecurity, Information Technology, Networking, Threat modeling.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 23 Edición No 02– Año 2024

INTRODUCCIÓN

En la última década los avances tecnológicos han permitido el advenimiento de nuevos productos y servicios relacionados con las tecnologías de IT, tales como las redes sociales, el Cloud Computing, el Big Data, el IoT (Internet Of Things), la AI (Artificial Intelligence) entre otras. Los constantes avances tecnológicos han generado una dependencia significativa a las TI para el funcionamiento adecuado de las organizaciones. Esta situación, ha sido aprovechada por delincuentes informáticos para realizar delitos como robo de información, espionaje industrial, robo de identidad, entre otras.

Debido a que la seguridad de la información es un área extensa y compleja de implementar debido a la gran cantidad de riesgos y tecnologías de seguridad en el mercado, se han desarrollado estándares internacionales para dar a las organizaciones una ruta a seguir para conseguir una postura robusta de seguridad. No obstante, para implementar este tipo de estándares es menester un análisis previo a la infraestructura tecnológica de la organización a fin de identificar la postura de seguridad de esta y su nivel de exposición a amenazas. Una parte importante de dicho análisis corresponde a la aplicación de una metodología de modelado de amenazas que devendrá en las estrategias de protección y corrección de errores a realizar sobre la plataforma tecnológica.

Tomando en consideración la diversidad de amenazas de ciberseguridad, así como el complejo proceso de adopción de estándares y controles de seguridad de la información para la protección de los datos de los usuarios en un ambiente heterogéneo de soluciones de IT, se plantea la siguiente interrogante, ¿Cómo se puede estructurar un enfoque metodológico que permita identificar, evaluar y mitigar amenazas en los entornos informáticos de empresas aseguradoras?

Para alcanzar estos objetivos, se analizan los resultados de investigaciones anteriores en materia de las metodologías de modelado de amenazas para identificar su focalización y metodologías de análisis para generar un modelo propio enfocado en las empresas aseguradoras. Seguidamente, se procede a validar el modelo a través de la identificación y caracterización de amenazas en la empresa seleccionada en los elementos de TI críticos para el negocio. Para esto se realizan entrevistas al personal de la empresa, y se analiza en mapa de red de esta para generar un mapa conceptual de las posibles explotaciones de las amenazas en la plataforma.

Es importante destacar que los mecanismos de recolección de información son la observación directa y la entrevista al personal de la organización. De igual forma, la naturaleza de los objetivos de selección de metodologías, así como la generación del modelo son de carácter cualitativo, cuyos indicadores son la protección de los activos críticos. Por su parte, el objetivo de validar el modelo es de tipo cuantitativo y sus indicadores son las vulnerabilidades y amenazas en los sistemas tecnológicos.

Fundamentación teórica

El análisis de riesgo representa una parte fundamental para elaborar una estrategia de ciberseguridad adecuada para las organizaciones. No obstante, dicho análisis requiere un proceso de modelado de amenazas en el cual se han de identificar los vectores de ataques a los sistemas informáticos y la metodología de explotación de las vulnerabilidades identificadas.

En este sentido, actualmente existen diversas metodologías de modelado de amenazas como Operational Critical, Threat, Asset and Vulnerability Evaluation (OCTAVE), Process for Attack

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 23 Edición No 02– Año 2024

Simulation and Threat Analysis (PASTA), National Institute of Standards and Technology (NIST), entre otras. Sin embargo, la calidad, consistencia, valor y cantidad de amenazas identificadas pueden variar significativamente para cada empresa según la metodología utilizada. Por lo que nuevos enfoques a esta temática han surgido a raíz de investigaciones en torno a las diversas formas de adoptar la metodología y análisis referentes a las acciones realizadas por los ciberdelincuentes para vulnerar e ingresar en los sistemas informáticos.

En este sentido, un enfoque centrado en el ciber atacante es propuesto por Cano (2020) cuya metodología de modelado de amenazas busca modelar al adversario y sus movimientos inesperados a partir de la incertidumbre para comprender mejor sus acciones. Este modelo, centrado en el ciberdelincuente, genera una capa de complejidad adicional al análisis al presuponer el perfil, objetivos y capacidades de este para la identificación de puntos ciegos en la dinámica de seguridad de las empresas; sin embargo, su enfoque permite identificar debilidades en los mecanismos de seguridad ante atacantes internos.

Por otra parte, Olivares, et al (2017) describe el modelado de amenazas enfocándose en un entorno de desarrollo de software seguro. Los autores concluyen que el éxito de un modelado de amenazas consiste en aplicarlo en múltiples ocasiones durante el desarrollo y evolución del proyecto. Así mismo, la metodología debe aplicarse a medida que se produzcan cambios en el entorno de la aplicación o sistema.

En el mismo orden de ideas, Solarte, et al (2015) en su artículo presenta los resultados obtenidos tras aplicar las fases de auditoría y evaluación de riesgos en un Sistemas de Gestión de Seguridad de la Información (SGSI) alineado con el estándar ISO/IEC 27001. Los autores concluyen que el proceso de auditoría de seguridad debe ser realizado de forma continua por los entes de control interno de la organización y de forma periódica por empresas de auditoría externa que permitan hacer la evaluación y el seguimiento del sistema de control de seguridad informática. Sus resultados exponen la falta de compromiso de la alta gerencia de las empresas con la implantación de estándares y controles de seguridad de la información.

Finalmente, Novoa, et al (2015), en su artículo presentan una descripción general de las metodologías de análisis de riesgo aplicadas en el ámbito de la seguridad informática para la concienciación de las organizaciones en su uso y la importancia de la integración del análisis de riesgo dentro de los SGSI. Los autores concluyen que la implementación de una metodología de análisis de riesgos permite identificar las vulnerabilidades y fortalezas de la organización por cada uno de sus activos informáticos. Así como también se logra identificar y valorar los procesos más críticos del negocio, determinar y evaluar las amenazas y su grado de efectividad.

Metodología

Esta investigación fue de tipo descriptiva y de campo ya que, analizó la Infraestructura Tecnológica de una empresa aseguradora ubicada en Caracas, Venezuela; la cual cuenta con diez sucursales a lo largo del territorio venezolano. La selección de este tipo de industria para esta investigación se debe a la gran importancia de la protección de la información de los usuarios del servicio, su homogeneidad en relación con el entorno tecnológico con otras empresas de este rubro en Latino América y de su estrecha relación con la banca.

Para seleccionar las metodologías para el desarrollo del modelado de Ciberamenazas, se recurre a la investigación bibliográfica para determinar el enfoque de las metodologías desarrolladas para el modelado de amenazas, sus puntos en común y diferencias para que sean

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 23 Edición No 02– Año 2024

utilizadas como base para el desarrollo de la metodología de este proyecto. Así mismo, para generar un modelo de análisis de Ciberamenazas se emplea la observación directa para determinar sí el modelo es útil para el descubrimiento de vectores de ataque en función de las variables de análisis identificadas.

Finalmente, Para validar el modelo de análisis, se estudia la superficie de ataque en los dispositivos críticos de la plataforma para identificar y caracterizar sus vulnerabilidades con la finalidad de desarrollar un diagrama conceptual que describa como estas amenazas pueden afectar la continuidad del negocio.

Análisis de los resultados

Para el desarrollo de este proyecto se han elegido tres metodologías de modelado de amenazas: PASTA, OCTAVE y NIST en base a que cada una de ellas realizan su función desde una perspectiva distinta del negocio. Las mismas se presentan en la tabla 1.

Tabla 1: Comparación de metodologías de modelado de amenazas.

Metodología	Descripción	Fases	Uso
OCTAVE	Se enfoca en riesgos organizacionales más que tecnológicos y consta de tres fases.	1. Crear perfiles de amenazas basados en activos 2. Identificar la vulnerabilidad de la infraestructura 3. Desarrollar una estrategia y planes de seguridad	Se orienta a la organización para que gestione sus evaluaciones de riesgo, tome decisiones basadas en estos, proteja los activos críticos y comunique la información efectivamente
PASTA	Es un proceso de siete pasos enfocado en alinear los requisitos técnicos de seguridad con los objetivos empresariales	1. Definir Objetivos 2. Definir alcance técnico 3. Descomposición de la aplicación 4. Análisis de amenazas 5. Análisis de vulnerabilidades y debilidades 6. Modelado de ataque 7. Análisis de riesgo e impacto	Se centra en los activos, el software y en la seguridad de los sistemas analizados
NIST	Es un proceso de cuatro pasos centrado en los datos de la organización	1. Identificar y caracterizar el sistema y datos de interés 2. Identificar y seleccionar los vectores de ataque a ser incluidos en el modelo 3. Caracterizar los controles de seguridad para mitigar los vectores de ataque 4. Analizar el modelo de amenazas	Se enfoca en los datos para generar el modelado de amenazas.

Fuente: Propia 2025.

Es esta, es importante destacar el enfoque de la metodología OCTAVE hacia la organización, por lo cual sus fases hacen referencia a la creación de perfiles para las amenazas permitiendo un análisis de riesgo basado en los objetivos del negocio.

Por otra parte, la metodología PASTA se enfoca en los activos de la organización identificando las amenazas potenciales a través de la descomposición de los sistemas (Hardware y Software) a analizar para identificar los riesgos potenciales en cada capa. Finalmente, NIST se enfoca en identificar los vectores de ataque y amenazas en función de los datos de una organización para asegurar la protección de estos.

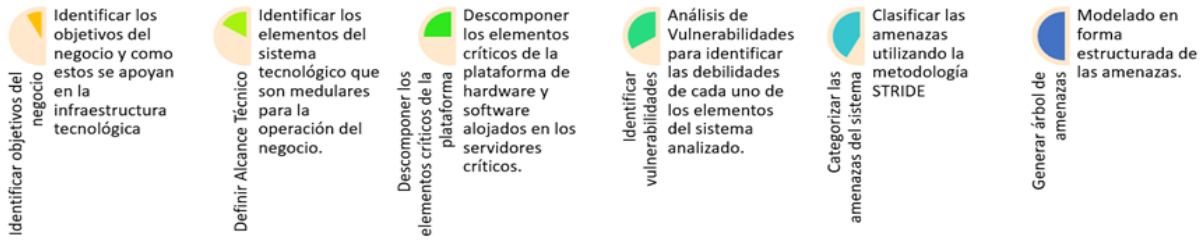
Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 23 Edición No 02– Año 2024

En otro orden de ideas, para generar un modelo de amenazas es importante considerar los sistemas que podrían verse afectados, comprender las acciones las acciones a tomar para reducir los riesgos, entre otras actividades; No obstante, es menester mencionar, como marco para esta tarea, los cinco pasos fundamentales de un modelo de amenazas según el Microsoft Security Development Lifecycle:

d)Definir los requerimientos de seguridad
e) Crear un diagrama de aplicación
f) Identificar amenazas
g) Mitigar amenazas, y
h) Validar que las amenazas hayan sido mitigadas

Tomando en cuenta los pilares de un modelado de amenazas, aunado a las fases de las metodologías NIST, PASTA y OCTAVE, se plantea una metodología de análisis que tome en cuenta los objetivos del negocio, los activos del negocio y vectores de ataque posibles. Por esto último, se considera como fuente para los riesgos, el informe presentado por Pwc en 2024. De acuerdo con este informe, la ciberseguridad es una de las preocupaciones más importantes para los CEO de empresas venezolanas; cuya preocupación principal radica en la perdida de datos, daños a la marca, pérdida de ingresos, caída de las operaciones, la afectación de la calidad y la perdida de propiedad intelectual. La figura 2 presenta el diagrama de secuencia de las fases de la metodología de modelado de amenazas definida.

Figura 2: Metodología de modelado de amenazas definida.



Fuente: Propia 2025.

A continuación, se describen las fases planteadas en la figura 1.

1. **Fase I. Identificar los objetivos del negocio:**

Identifica los objetivos a largo, mediano y corto plazo del negocio a través de entrevistas con el personal de la alta gerencia de la organización con el objetivo de identificar los elementos del entorno tecnológico se alinean con los objetivos definidos.

2. **Fase II. Definir Alcance Técnico:**

Identifica los procesos y activos del sistema tecnológico que son críticos para la operación del negocio y sus objetivos a través de entrevistas con el personal técnico de la organización, aunado al análisis de su entorno tecnológico y de ciberseguridad.

3. **Fase III. Descomponer los elementos críticos de la plataforma**:

Estriba en descomponer los elementos de Hardware y Software, medulares para los objetivos de la organización y para el negocio, en sus elementos más básicos con el objetivo de facilitar el análisis de brechas de seguridad de cada elemento por separado.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 23 Edición No 02– Año 2024

4. **Fase IV. Identificar vulnerabilidades en los sistemas analizados**

Consiste en realizar análisis de vulnerabilidades para identificar las amenazas en cada uno de los elementos analizados a través de herramientas especializadas para este fin en la red interna, y realizando búsquedas en internet relacionadas con la empresa para identificar brechas de seguridad que puedan ser identificadas fácilmente por los Ciberdelincuentes.

5. **Fase V. "Categorizar las amenazas del sistema"**

Consiste en clasificar las amenazas, derivadas de las vulnerabilidades identificadas, e identificar los riesgos e impacto que estas presentan para la infraestructura tecnológica, a través del empleo de la herramienta de análisis STRIDE.

6. **Fase VI. Generar los mapas de ataques de las amenazas identificadas:**

Radica en la creación de los diagramas conceptuales que describen el desarrollo de los ataques que puedan explotar las vulnerabilidades identificadas en los activos críticos, y cómo estas afectan la continuidad del negocio y los objetivos planteados por la organización.

A continuación, se valida la metodología planteada en la figura 1, por medio de la aplicación de esta. Para el desarrollo de las fases I y II de la metodología, se realizaron entrevistas al personal de la Gerencia de Tecnología de la organización para determinar los objetivos del negocio y los sistemas de TI medulares para la organización. Los resultados obtenidos se presentan en la tabla 3.

Tabla 3: Comparación de metodologías de modelado de amenazas.

Servicio	Servidor	Función	Criticidad (Escala: 1 a 10)
SIR	SIR Aplicaciones	Almacenan los aplicativos del negocio	10
	SIR Data Base	Almacena las bases de datos de los clientes del negocio	10
Portales de servicios WEB	Portal de Centro Operativo	Portal de emisión de pólizas centralizado	10
	Portal de Productores	Utilizado para que los productores y corredores accedan a la información de sus clientes	10
	Portal de Botón de pago	Portal para que los clientes realicen sus pagos de forma online	10

Fuente: Propia 2025.

En la tabla 3, se identifican los elementos de TI medulares para la compañía, siendo estos el SIR y los portales WEB que optimizan los procesos de la organización. Los portales de "Centro Operativo" y "Productores" se alojan en un solo servidor y el servicio de "Portal de Botón de Pago" se aloja en un servidor distinto. El servidor "SIR" no se publica a internet.

Estos elementos son críticos para el negocio debido a que agilizan los tiempos de respuestas ante la solicitud de emisión de pólizas para los clientes, facilita los medios de pago y apoya a los corredores para conseguir información para sus clientes de forma rápida. En cuanto a la postura de seguridad de la empresa, esta no cuenta con una metodología para facilitar la creación de una matriz de riesgo y, al mismo tiempo, les permita generar un plan de mitigación ante amenazas. Esto último provoca la reactividad de los mecanismos de respuestas ante incidentes.

A continuación, se desarrolla la fase III de la metodología presentada en la que se descomponen los dispositivos medulares de la organización en sus elementos más básicos para

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 23 Edición No 02– Año 2024

analizar sus vulnerabilidades e identificar sus amenazas. Para realizar este análisis se descomponen estos dispositivos en:

a) Servicios de datos
b) Hardware y Software

La tabla 4 presenta la descomposición de los elementos de los servidores utilizados para la publicación de los portales WEB y del servidor SIR. De la información recopilada es posible determinar que la organización emplea una arquitectura de servicios obsoleta, así como también cuenta con diversas vulnerabilidades tanto a nivel de sistema operativo como de los aplicativos utilizados para poner en funcionamiento la operación del negocio.

Tabla 4: Comparación de metodologías de modelado de amenazas.

Servidor	Aplicaciones	Protocolos de Conexión	Sistema Operativo
SIR Aplicaciones	Oracle application server 10.1.2.3	SSH	AIX 5.3
SIR Data Base	Oracle 10.2.0.4	SSH	AIX 7.1
Portal de Centro Operativo y Portal de Productores	Oracle 11g	SSH	SUSE Linux 11
Portal de Botón de pago	WampServer 2.2 Apache 7.0 Oracle 11g MySQL Tool 5.0 MySQL Connector 6.7 Microsoft Web Platform 4.6 Open SSL 1.01	LDAP	Windows 2008 R2 Standard

Fuente: Propia 2025.

A continuación, se desarrolla la fase IV de la metodología planteada al analizar las vulnerabilidades de los sistemas de TI críticos para la empresa. La tabla 5 presenta los hallazgos identificados al escanear los recursos publicados de la empresa a través de internet. Las vulnerabilidades presentadas son todas aquellas que cuenten con una puntuación de 7 o superior en la escala de CVSS v2.0.

Tabla 5: Vulnerabilidades identificadas desde internet.

CVE	CVSS Score	Riesgo	Servicio	Protocolo	Puerto	Nombre	Descripción
CVE-2010-2965	10	Crítico	Portal de Centro Operativo y Portal de Productores	udp	17185	*VxWorks WDB Debug Service Detection*	Pueden utilizarse comandos arbitrarios en este puerto
	10	Crítico	Portal de Botón de pago	udp	17185	*VxWorks WDB Debug Service Detection*	Pueden utilizarse comandos arbitrarios en este puerto
CVE-2018-15355	7.1	Alto	Portal de Botón de pago	tcp	143	*SSL Version 2 and 3 Protocol Detection*	El servicio encripta información usando un protocolo con vulnerabilidades conocidas

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 23 Edición No 02– Año 2024

	7.1	Alto	Portal de Botón de pago	tcp	443	*SSL Version 2 and 3 Protocol Detection*	El servicio encripta información usando un protocolo con vulnerabilidades conocidas
	7.1	Alto	Portal de Botón de pago	tcp	993	*SSL Version 2 and 3 Protocol Detection*	El servicio encripta información usando un protocolo con vulnerabilidades conocidas
-	7.5	Alto	Portal de Botón de pago	tcp	443	*Unsupported Web Server Detection*	El servidor WEB es obsoleto
-	10	Crítico	Portal de Botón de pago	tcp	443	*Microsoft Exchange Server Unsupported Version Detection*	El servidor Exchange está fuera de soporte

Fuente: Propia 2025.

La tabla 6 presenta las vulnerabilidades identificadas en los servidores debido a los aplicativos y sistema operativo instalado. Es importante destacar que todos los aplicativos y sistemas operativos listados están obsoletos, por lo tanto, es menester actualizar estos sistemas. Por esto último se han seleccionado aleatoriamente vulnerabilidades inherentes a estos softwares, la severidad indicada corresponde a la ponderación CVSS v2.0.

Tabla 6: Vulnerabilidades identidades en los aplicativos presentes en los activos críticos.

Aplicativo	Vulnerabilidad	CVSS Score	Descripción
WampServer 2.2	CVE-2019-11517	5.8	WampServer antes de 3.1.9 tiene CSRF en add_vhost.php porque el patrón de sincronizador implementado como corrección de CVE-2018-8817 estaba incompleto. Un atacante podría agregar / eliminar cualquier vhosts sin el consentimiento del propietario.
Oracle 11g	CVE-2009-0985	7.1	La vulnerabilidad no especificada en el componente Core RDBMS en Oracle Database 10.1.0.5, 10.2.0.4 y 11.1.0.6 permite que los usuarios autenticados de forma remota con el rol IMP_FULL_DATABASE afecten la confidencialidad, integridad y disponibilidad.
Apache 7.0	CVE-2010-4476	5.0	Un error de JVM podría hacer que Double conversion cuelgue la JVM al acceder a una página con restricciones de seguridad basada en formularios o cualquier página que llame a javax.servlet.ServletRequest.getLocale () o javax.servlet.ServletRequest.getLocales (). Se puede utilizar una solicitud especialmente diseñada para desencadenar una denegación de servicio.
MySQL Tool 5.0	CVE-2007-2583	4.0	La función in_decimal :: set en item_cmpfunc.cc en MySQL antes de 5.0.40 y 5.1 antes de 5.1.18-beta, permite a los atacantes dependientes del contexto causar una denegación de servicio (bloqueo) a través de una cláusula IF diseñada que da como resultado una división -por-cero error y una desreferencia del puntero NULO.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 23 Edición No 02– Año 2024

MySQL Connector 6.7	CVE-2019-2435	5.8	Vulnerabilidad en el componente MySQL Connectors de Oracle MySQL (subcomponente: Connector / Python). Las versiones compatibles que se ven afectadas son 8.0.13 y anteriores y 2.1.8 y anteriores. La vulnerabilidad fácilmente explotable permite que un atacante no autenticado con acceso a la red a través de TLS comprometa los conectores MySQL. Los ataques exitosos requieren la interacción humana de una persona que no sea el atacante. Los ataques exitosos de esta vulnerabilidad pueden resultar en el acceso no autorizado de creación, eliminación o modificación a datos críticos o todos los datos accesibles de MySQL Connectors, así como acceso no autorizado a datos críticos o acceso completo a todos los datos accesibles de MySQL Connectors. CVSS 3.0 Base Score 8.1 (impactos de confidencialidad e integridad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: N / UI: R / S: U / C: H / I: H / A: N).
Microsoft Web Platform 4.6	CVE-2020-1476	2.1	Existe una vulnerabilidad de elevación de privilegios cuando las aplicaciones web ASP.NET o .NET que se ejecutan en IIS permiten incorrectamente el acceso a los archivos almacenados en caché. Un atacante que aproveche con éxito esta vulnerabilidad podría obtener acceso a archivos restringidos. Para aprovechar esta vulnerabilidad, un atacante debería enviar una solicitud especialmente diseñada a un servidor afectado.
Open SSL 1.01	CVE-2016-6304	7.8	Múltiples fugas de memoria en t1_lib.c en OpenSSL antes de 1.0.1u, 1.0.2 antes de 1.0.2i y 1.1.0 antes de 1.1.0a permite que atacantes remotos provoquen una denegación de servicio (consumo de memoria) a través de grandes extensiones de solicitud de estado OCSP.
Oracle 10.2.0.4	CVE-2012-3220	9.0	La vulnerabilidad no especificada en el componente espacial en Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 y 11.2.0.3 permite que los usuarios autenticados de forma remota con privilegios de Crear sesión afecten la confidencialidad, integridad y disponibilidad a través de vectores desconocidos.
Oracle application server 10.1.2.3	CVE-2008-4017	5.0	La vulnerabilidad no especificada en el componente OC4J en Oracle Application Server 10.1.2.3 permite a atacantes remotos afectar la confidencialidad a través de vectores desconocidos.
AIX 7.1	CVE-2018-1383	9.0	Un error de lógica de software crea una vulnerabilidad en un demonio AIX 6.1, 7.1 y 7.2 que podría permitir a un usuario con privilegios de root en un sistema obtener acceso de root en otra máquina.
AIX 5.3	CVE-2010-0922	7.8	La vulnerabilidad no especificada en secldapclntd en IBM AIX 5.3 con SP 5300-11-02 permite a los atacantes causar una denegación de servicio (falla de inicio de sesión LDAP) a través de vectores desconocidos. NOTA: algunos de estos detalles se obtienen de información de terceros.
SUSE Linux 11	CVE-2009-1648	7.5	The YaST2 LDAP module in yast2-ldap-server on SUSE Linux Enterprise Server 11 (aka SLE11) does not enable the firewall in certain circumstances involving reboots during online updates, which makes it easier for remote attackers to access network services.
Windows 2008 R2 Standard	CVE-2020-17051	10.0	Vulnerabilidad de ejecución remota de código del sistema de archivos de red de Windows

Fuente: Propia 2025.

A continuación, se desarrolla la fase V de la metodología la cual se enfoca en la categorización de las amenazas a través de la metodología STRIDE. El resultado de la caracterización se presenta en la tabla 7. Esta describe las amenazas detectadas a través del análisis de las vulnerabilidades identificadas en los aplicativos y sistemas operativos de los servidores críticos para la organización.

De las amenazas identificadas utilizando la metodología STRIDE, se destaca la presencia de siete amenazas de “Denial of Services” y seis de “Elevation of Privileges” las cuales son las

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 23 Edición No 02– Año 2024

amenazas más recurrentes. Por otra parte, se identificaron tres amenazas correspondientes a "Tampering", tres amenazas de "Information Displosure" y solo una relacionada con el "Spoofing". Finalmente, es importante mencionar que el método de conexión al portal de Botón de pago se realiza a través del protocolo LDAP el cual es inseguro al no encriptar la información relacionada con el usuario y contraseña en tránsito por la red LAN permitiendo el acceso de un atacante a esta información.

Tabla 6: Caracterización de las amenazas identificadas en los activos críticos analizados.

Vulnerabilidad	STRIDE	Amenaza
CVE-2010-2965	Spoofing Denial of Service Tampering	Permite al atacante llamar funciones y ejecutar tareas
CVE-2018-15355	Information disclosure	Permite descifrar de datos transmitidos
CVE-2019-11517	Denial of Service Elevation of Privilege	Permite eliminar host virtuales dentro del sistema de virtualización
CVE-2009-0985	Elevation of Privilege	Permite acceder a información sensible dentro de la base de datos
CVE-2010-4476	Denial of Service	Permite al atacante causar un estado de Denegación de Servicios
CVE-2007-2583	Denial of Service	Permite al atacante causar un estado de Denegación de Servicios
CVE-2019-2435	Denial of Service Elevation of Privilege Tampering	Permite al atacante crear, modificar o eliminar información.
CVE-2020-1476	Elevation of Privilege	Permite al atacante elevar sus privilegios en el sistema
CVE-2016-6304	Denial of Service	Permite al atacante causar un estado de Denegación de Servicios
CVE-2008-4017	Information disclosure	Permite acceder a información sensible dentro de la base de datos
CVE-2012-3220	Elevation of Privilege	Permite al atacante elevar sus privilegios en el sistema
CVE-2018-1383	Elevation of Privilege	Permite al atacante elevar sus privilegios en el sistema
CVE-2010-0922	Denial of Service	Permite al atacante causar un estado de Denegación de Servicios
CVE-2009-1648	Information disclosure	El atacante puede acceder al servidor a través de los servicios de red por la deshabilitación temporal del firewall
CVE-2020-17051	Elevation of Privilege Information disclosure Tampering	Vulnerabilidad de ejecución remota de código del sistema de archivos de red de Windows.

Fuente: Propia 2025.

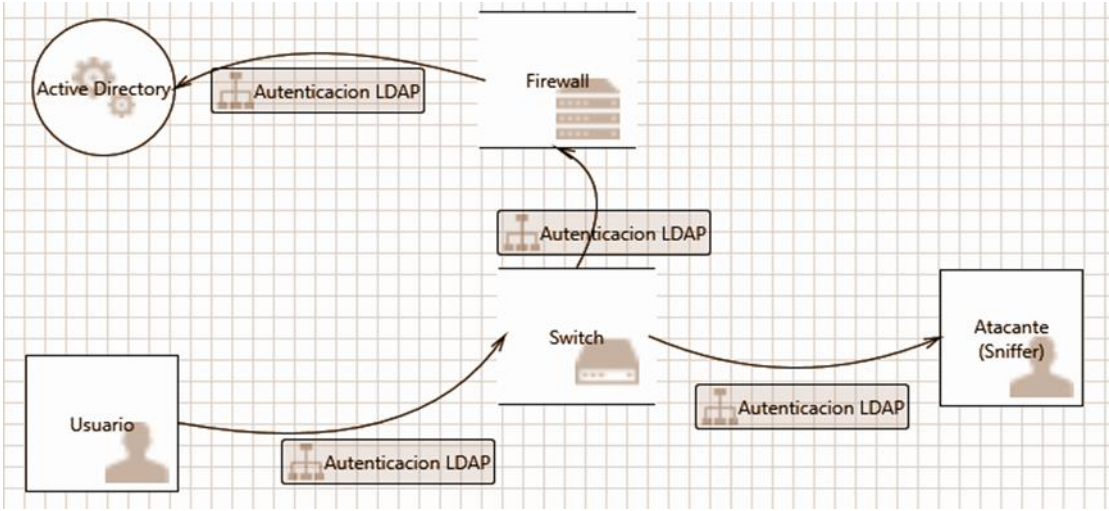
Todo lo anterior converge en la fase VI de la metodología, donde se desarrollan los mapas conceptuales de los ataques que busquen explotar las vulnerabilidades listadas en la tabla 6. Para este inciso se desarrolla un solo mapa conceptual, específicamente el relacionado a la amenaza del robo de credenciales a través de la red debido a la debilidad del protocolo de comunicación LDAP, el cual es utilizado para acceder a los PCs y Servidores del dominio de la organización. Dicho mapa se presenta en la figura 3.

La figura 3 presenta el proceso de conexión entre un usuario del dominio y el servidor del Directorio Activo (AD). Cada usuario debe acceder al AD para validar sus credenciales y acceder a su PC u otro recurso compartido dentro del dominio de la organización. El diagrama presenta la amenaza de un "Hombre en el Medio" (Man in The Middle), donde un usuario malintencionado consigue capturar tráfico de la red de la organización a través de un Sniffer. En este caso, todas

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 23 Edición No 02– Año 2024

las comunicaciones entre el servidor AD y el usuario serían interceptadas por el usuario malintencionado si no se utiliza cifrado TLS/SSL; esto le permite al atacante acceder a la contraseña y usuario del personal de la empresa. Esta metodología de trabajo debe ser aplicada a todas las amenazas detectadas a fin de proveer de toda la información posible al departamento pertinente para crear estrategias de gestión de riesgos determinar las estrategias de mitigación pertinentes.

Figura 3: Mapa de ataques de una amenaza de MitM por protocolo LDAP sin encriptación.



Fuente: Propia 2025

Conclusiones

En conclusión, las tecnologías de comunicaciones son una herramienta fundamental para los negocios, donde los que no cuenten con estrategias de mercado enfocadas en la era digital están destinados a desaparecer. No obstante, el uso de estas tecnologías atrae a los Ciberdelincuentes, quienes están en constante búsqueda de nuevas oportunidades de lucro en base a actividades malintencionadas. Por esto último, los procesos de seguridad de la información son una pieza fundamental para la defensa de las organizaciones.

Estos procesos buscan resguardar la infraestructura tecnológica de la organización a través de la implementación procesos de seguridad. No obstante, estos deben ser implementados en base a metodologías apropiadas que permitan identificar y mitigar los riesgos en la arquitectura tecnológica de la organización y generar estrategias de resiliencia en base a los riesgos críticos para el negocio.

En este sentido, este proyecto presentó una metodología de modelado de amenazas para ser utilizado en conjunto con técnicas de análisis de riesgo, a fin de identificar las amenazas sobre una arquitectura tecnológica en empresas aseguradoras. Todo esto en base a sus objetivos de negocio y un análisis profundo de los elementos fundamentales que componen los aplicativos medulares para una organización.

Los resultados obtenidos les permiten a las organizaciones visualizar las fases de un ataque informático, así como su caracterización y criticidad en función de los procesos del negocio. La

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 23 Edición No 02– Año 2024

aplicación continua de esta herramienta facilita el análisis de gestión de riesgos, requeridos por la normativa ISO/IEC 27000, entre otras, al elaborar una base de datos de tipos de los diversos tipos de ataque a los que pueden ser vulnerable un elemento en específico de la plataforma tecnológica. Se recomienda que esta sea aplicada con cada cambio realizado para actualizar constantemente la base de riesgos de la organización.

Finalmente, esta metodología toma como punto de referencia una empresa aseguradora venezolana; no obstante, puede ser implementada en cualquier empresa aseguradora a nivel latinoamericano, debido a la homogeneidad tecnológica que existe entre las organizaciones de este rubro en la región.

Referencias Bibliográficas

- Hutchins, E. (2011). Intelligence-Driven Computer network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, 6th International Conference on I-Warfare and Security.
- Cano, J. (2020). Modelo SOCIA. Una reflexión conceptual y práctica desde la perspectiva del adversario. X Congreso Iberoamericano de Seguridad Informática.
- Olivares, B. (2017) Modelado de amenazas, una técnica de análisis y gestión de riesgo asociado a software y aplicaciones. Universidad Piloto de Colombia.
- Solarte, F. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica ESPOL – RTE, Vol. 28.
- Novoa, H. (2015). Metodologías para el análisis de riesgos en los SGSI. Revista especializada en Ingeniería, Vol. 9.
- Project Management Institute (2017), Guía de los Fundamentos para la Dirección de Proyectos 6ª edición, EE. UU.
- Rodríguez, E. (2005) Metodología de la Investigación. Universidad autónoma de Tabasco.
- MAPFRE Economics (2020), El Mercado Asegurador Latinoamericano en 2019, Madrid, Fundación MAPFRE.
- Microsoft, Threat Modeling, (Online). Disponible en: https://tinyurl.com/2648dr3v
- Pwc, Redefiniendo la estrategia para hacer frente a los ciberataques (Online). Disponible en: https://tinyurl.com/2dda9lrv
- National Institute of Standards and Technology (2016), Guide to Data-Centric System Threat modeling. United States.
- OWASP Foundation (2011), Threat Modeling of Banking malware-Based Attacks (Online). Disponible en: https://tinyurl.com/2bm66qab
- Martínez, M (2019). Análisis y comparación de herramientas de análisis de amenazas. Universidad Carlos III de Madrid
- Martínez, M (2019). Análisis y comparación de herramientas de análisis de amenazas. Universidad Carlos III de Madrid

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 23 Edición No 02– Año 2024