# Tesis de Maestría

## Modelo de seguridad para la gestión de vulnerabilidades de servidores en Nubes privadas


EMISI

Maestría en Ingeniería en Sistemas de Información

Universidad Tecnológica Nacional

Facultad Regional Santa Fe

**Autor:** Ing. Simón A. Cifre

**Director:** Dr. Jorge Roa

**Co-Director:** Dr. Emiliano Reynares



Año 2020

## Resumen

Las organizaciones deben asegurar sus infraestructuras de Nube privada en un actual entorno volátil y de rápido movimiento, que se caracteriza por una proliferación de amenazas y vulnerabilidades que constantemente intentan emerger y afectar. Los piratas informáticos y los adversarios aprovechan continuamente las tecnologías de punta para explotar la creciente cantidad de vulnerabilidades de los activos físicos y cibernéticos de las infraestructuras críticas. Por lo tanto, no es práctico y, en varios casos, no es posible llevar a cabo manualmente todas las tareas de seguridad y protección, tales como actividades de detección de amenazas, actualizaciones, monitoreo, informes y aplicación de políticas de seguridad.

Para evitar los costosos y exigentes resultados de los análisis de vulnerabilidades, falsos positivos, evaluaciones parciales de los sistemas y métodos de mitigación ineficientes, es necesario aplicar un proceso de gestión de vulnerabilidades. El verdadero valor agregado de estas evaluaciones se produce cuando las mismas están integradas a un proceso de gestión de vulnerabilidades.

Un proceso completo y eficiente de gestión de vulnerabilidades debe desplegarse a partir de un modelo de seguridad, alineado a estándares internacionales de seguridad, con una política de seguridad específica que contemple un proceso de aseguramiento de activos, lineamientos de operación, roles de usuarios, documentación requerida, un conjunto de indicadores de vulnerabilidad y clasificadores de madurez organizacional.

La presente tesis de maestría tiene como objetivo principal definir un modelo de seguridad para gestión de vulnerabilidades de servidores en Nubes privadas, que contemple lineamientos generales para el diseño de una política de seguridad donde se detallen roles de usuarios y documentación recomendada, un proceso de aseguramiento apoyado sobre actualizaciones, indicadores de vulnerabilidad basado en factores críticos de seguridad, y clasificación de niveles de seguridad fundamentada en la madurez de la organización. El propósito es proponer especificaciones concretas de las actividades que se deben llevar a cabo para realizar una adecuada gestión de vulnerabilidades siguiendo los lineamientos de los estándares internacionales ISO/IEC 27000 y O-ISM3, facilitando el proceso de

certificación de ISO/IEC 27001 por parte de las organizaciones.

## Contenido

# 1. Introducción

Existen diversos avances tecnológicos que están impulsando la transformación digital de las organizaciones y uno de los casos más destacados es la Computación en la Nube [1]. Cada año son más las organizaciones que confían en la Nube para sus datos. La Computación en la Nube ha pasado de ser un avance tecnológico a una parte fundamental de la estrategia tecnológica de las organizaciones. Hoy en día, gran parte de las cargas de trabajo empresariales ya se están ejecutando en la Nube y se estima que seguirá en aumento [2].

Existen numerosos casos a nivel mundial de organizaciones importantes y prestigiosas que fueron víctimas de ataques informáticos filtrados mediante vulnerabilidades en los sistemas operativos y software instalados en los servidores. Durante el año 2018 se identificó un incremento del 27% de vulnerabilidades de seguridad publicadas respecto a 2017, la cantidad de ataques informáticos creció en un 58% comparando los mismos años, y generó sólo en 2018 pérdidas económicas por más de mil millones de dólares, de acuerdo al informe de inteligencia de Tenable [3]. Uno de los principales motivos que permiten y facilitan los ataques de hackers es la existencia de vulnerabilidades. Al tratarse de entornos de software, es importante que los sistemas se actualicen con las últimas versiones que hayan sido validadas como correctas, para evitar ataques apoyados en posibles vulnerabilidades conocidas [4].

Se detectó, además, que los atacantes disponen de una ventana de oportunidad de 3 a 7 días para efectuar un ataque, aprovechando una vulnerabilidad funcional no descubierta. La brecha resultante de días está directamente relacionada con la forma en la que las organizaciones realizan el proceso de gestión de vulnerabilidades, desde el análisis y detección de la amenaza hasta su mitigación [5].

Actualmente son muchas las organizaciones que migran sus servicios con servidores en centros de datos locales a esquemas de computación en Nubes privadas. Sin embargo, adoptar una infraestructura de Nube privada comparte múltiples riesgos con servidores en centros de datos locales, como los asociados a seguridad y los desafíos de mantenimiento [6]. Los proveedores de servicios de Nubes privadas proporcionan una primera línea de

defensa al actualizar sus infraestructuras y servicios, pero los clientes tienen un papel que desempeñar en la identificación y actualización de servidores y software vulnerables, y para esto es necesario contar con herramientas de exploración de vulnerabilidades y con un modelo de análisis de seguridad diseñado para arquitecturas basadas en la Nube [4].

Frente a los avanzados y heterogéneos entornos de tecnologías de la información y la lista creciente de posibles problemas en la seguridad, las organizaciones se encuentran con múltiples inconvenientes al momento de ocuparse de todas las vulnerabilidades conocidas. Debido al elevado número de revisiones de actualización distribuidas y a la dificultad de cuantificar el valor de las reparaciones de seguridad para los gerentes de las organizaciones, la mitigación de las debilidades de sistemas operativos y aplicaciones fundamentales es un reto constante [7].

Son muchas las organizaciones que actualmente utilizan herramientas para realizar análisis de vulnerabilidades e instalan actualizaciones de seguridad de manera independiente y aislada. Sin embargo, sin un proceso de gestión de vulnerabilidades que ayude a integrar y organizar las tareas de corrección, las organizaciones pueden directamente no aplicar acciones preventivas frente a los ataques basados en vulnerabilidades. Los estándares internacionales de seguridad de la información más aplicados en las organizaciones a nivel mundial son ISO/IEC 27000 y O-ISM3 [8]. El estándar ISO/IEC 27000 es un conjunto de normas desarrolladas por ISO e IEC que proporcionan un marco de gestión de la seguridad de la información y define un conjunto de buenas prácticas asociadas a la gestión de vulnerabilidades técnicas dentro del dominio de seguridad operativa [9]. Por otro lado, O-ISM3 es un estándar de madurez de seguridad de la información orientado a procesos que permite que las organizaciones puedan focalizarse sobre la adecuada administración de políticas, procesos, métricas y controles de seguridad para mitigar los riesgos sobre sus equipos informáticos [10].

Desde hace un tiempo, a partir del desarrollo y difusión de diversas regulaciones internacionales, estándares y buenas prácticas, las organizaciones han ido tomando cada vez mayor conciencia de la importancia de realizar evaluaciones de vulnerabilidades y/o test de intrusiones. Estos estándares o regulaciones recomiendan o exigen la ejecución en forma

regular de cierta cantidad de análisis de vulnerabilidades o test de intrusiones en forma periódica [11]. Dentro del conjunto de buenas prácticas que ofrecen, tanto ISO/IEC 27000 y O-ISM3 destacan la necesidad de obtener un inventario de todos los servidores como así también de las aplicaciones instaladas, utilizar buscadores de vulnerabilidades, determinar niveles de riesgo y reparar los sistemas o dispositivos vulnerables.

Para evitar los costosos y exigentes resultados de los análisis de vulnerabilidades, falsos positivos, evaluaciones parciales de los sistemas y métodos de mitigación ineficientes, es necesario aplicar un proceso de gestión de vulnerabilidades. El verdadero valor agregado de estas evaluaciones se produce cuando las mismas están integradas a un proceso de gestión de vulnerabilidades [11]. Sin dicho proceso no es posible dar cumplimiento a los requerimientos establecidos por diversos estándares y regulaciones del mercado [7].

Actualmente existen distintas soluciones de seguridad que ofrecen un sistema de gestión de vulnerabilidades [12][13][14]. Además, se detectan distintos trabajos de investigación relacionados con la seguridad en servidores y en la computación en la nube, aunque todos estos presentan limitaciones importantes [15][16][17][18][19]. La mayoría de las limitaciones se centran en versiones específicas de sistemas operativos y aplicaciones, no se ajustan a una política de seguridad organizacional, no disponen de mecanismo de monitoreo, no se alinean a algún estándar de seguridad, presentan sólo recomendaciones generales, no visualizan la importancia de la gestión de vulnerabilidades y no definen procesos operacionales.

De este modo, en la presente tesis de maestría se propone un proceso completo y eficiente de gestión de vulnerabilidades desplegado a partir de un modelo de seguridad, con una política de seguridad específica asociado a actualizaciones de seguridad que definen lineamientos de operación, roles de usuarios, documentación requerida, un conjunto de indicadores de vulnerabilidad y clasificadores de madurez organizacional. Se espera que el modelo de seguridad sea transversal a todas las capas de servidores en Nube privada y que por lo tanto, permita asegurar las vulnerabilidades a nivel operativo, de servicios, y de aplicaciones y software.

La investigación del tema abordado inició como trabajo final de integración de la

carrera Especialización en Ingeniería en Sistemas de Información de UTN Facultad Regional Santa Fe [20], con el título "Marco de trabajo estructurado para la seguridad de la información en servidores basado en estándares internacionales", aprobado el 12 de Noviembre de 2018. Además, se presentó un trabajo [21] en las 48° JAIIO (Jornadas Argentinas de Informática) dentro del simposio IETF Day 2019 – Taller del Grupo de Trabajo de Ingeniería de Internet, con el título "Gestión y operación de seguridad en servidores Web basadas en ISO/IEC27000 y O-ISM3" que fue aprobado con fecha de presentación el 16 de Septiembre de 2019 en la ciudad de Salta, Argentina.

A continuación, se presenta la estructura del presente informe. La Sección 2 detalla el estado actual de la computación en la nube y su seguridad, vulnerabilidades informáticas y mitigaciones, ataques informáticos y soluciones existentes con sus limitaciones. La Sección 3 describe los estándares internacionales de seguridad de la información ISO/IEC 27000 y O-ISM3 con sus clasificaciones, beneficios y limitaciones que lo caracterizan. Además, se presenta el Marco de trabajo de seguridad de la información construido como TFI a partir de los estándares mencionados, con sus módulos y controles. La Sección 4 detalla el modelo de seguridad con sus características propuesto en la presente tesis de maestría. La Sección 5 demuestra un caso de implementación del modelo de seguridad expuesto en la sección anterior. A continuación, la Sección 6 concluye sobre la propuesta del modelo con sus beneficios. Finalmente, la Sección 7, presenta un detalle de los trabajos futuros.

# 2. Contexto

## 2.1. Computación en la Nube y Seguridad

En el campo de la informática y las telecomunicaciones, por servidor se entiende un equipo informático que forma parte de una red y provee servicios a otros equipos, que reciben el nombre de clientes [22]. Generalmente los servidores son de uso dedicado, es decir, brindan un servicio o una pequeña cantidad de servicios en particular [23]. Existen diversos tipos de servidores, y su clasificación varía teniendo en cuenta tecnología de

implementación, servicio que brinda, función y contenido, principalmente.

La clasificación de los servidores es independientemente del modelo y de las tecnologías de información con la que se implementó, y se destacan [23] [24]: Servidor de archivos, Servidor de correo, Servidor de base de datos, Servidor de seguridad, Servidor Web, Servidor de impresiones, Servidor de fax, Servidor de telefonía, Servidor proxy, Servidor de acceso remoto (RAS), Servidor de DNS, Servidor de DHCP, Servidor de FTP, Servidor de chat, Servidor de imágenes y Servidor de audio/video.

En el modelo tradicional de implementación de un servidor, las organizaciones destinan recursos materiales, humanos y tecnológicos, los cuales se agrupan en un área encargada de solucionar los problemas relacionados con la infraestructura informática y el desarrollo de aplicaciones para la organización [25]. Allí, la mayoría de dichas áreas, se ven obligadas a dedicar una buena parte de su tiempo en las tareas de implementar, configurar, dar mantenimiento y actualizar proyectos relacionados con la infraestructura de su organización [25].

A partir de los avances tecnológicos de los últimos años, en la actualidad existe la posibilidad de trabajar con servidores en Nube. Este tipo de servidor es virtual, es decir que, mediante software con una infraestructura redundante alojada en un datacenter del proveedor, la ejecución de las tareas se distribuye entre un conjunto de máquinas físicas. Esto quiere decir que, si un dispositivo físico falla, el servicio sigue funcionando con total normalidad, ya que los datos no dependen de un solo equipo.

La Computación en la Nube es un modelo para permitir el acceso ubicuo, confiable y bajo demanda a un conjunto compartido de recursos informáticos configurables que pueden aprovisionarse y liberarse rápidamente con un mínimo esfuerzo de administración o interacción con el proveedor de servicios [26].

La nube no es un lugar, sino un método de gestión de recursos de TI que reemplaza las máquinas locales y los centros de datos privados con infraestructura virtual. En este modelo, los usuarios acceden a los recursos virtuales de computación, red y almacenamiento que están disponibles en línea a través de un proveedor remoto. Estos recursos se pueden

aprovisionar de manera instantánea, lo que es particularmente útil para las organizaciones que necesitan escalar verticalmente su infraestructura o reducirla rápidamente en respuesta a una demanda fluctuante [27].

El modelo de Computación en la Nube presenta cinco características esenciales, de acuerdo a NIST [26]: Auto servicio a demanda, Amplio acceso a la red, Puesta en común de recursos, Elasticidad rápida y Servicio medido. Además, los tipos de implementación en la Nube se caracterizan por el modelo de servicio como así también por el modelo de despliegue.

### 2.1.1. Modelos de servicio

El modelo de Computación en la Nube presenta al menos tres modelos de servicio, como se observa en la Figura 1, y los destacados son [26]:

- El software como servicio (SaaS). La capacidad provista al consumidor es utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura en la nube. Se puede acceder a las aplicaciones desde varios dispositivos cliente a través de una interfaz de cliente ligero, como un navegador web (por ejemplo, correo electrónico basado en web) o una interfaz de programa. El consumidor no administra ni controla la infraestructura de la nube subyacente, incluidas la red, los servidores, los sistemas operativos, el almacenamiento o incluso las capacidades de las aplicaciones individuales, con la posible excepción de los ajustes de configuración de aplicaciones específicos de usuarios limitados.
- Plataforma como servicio (PaaS). La capacidad provista al consumidor es implementar en la infraestructura en la nube las aplicaciones creadas o adquiridas por el consumidor mediante lenguajes de programación, bibliotecas, servicios y herramientas compatibles con el proveedor. El consumidor no administra ni controla la infraestructura en la nube subyacente, incluida la red, servidores, sistemas operativos o almacenamiento, pero tiene control sobre las aplicaciones implementadas y posiblemente los ajustes de configuración para el entorno de alojamiento de aplicaciones.

- Infraestructura como servicio (IaaS). La capacidad que se brinda al consumidor es proporcionar recursos de procesamiento, almacenamiento, redes y otros recursos informáticos fundamentales donde el consumidor puede implementar y ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones. El consumidor no administra ni controla la infraestructura de la nube subyacente, pero tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones implementadas; y posiblemente control limitado de componentes de red seleccionados (por ejemplo, servidores de seguridad de host).


**Figura 1.** Relación entre modelos de servicio.

### 2.1.2. Modelos de despliegue

El modelo de Computación en la Nube presenta cuatro modelos de implementación [26]:

- Nube privada. La infraestructura en la nube se proporciona para uso exclusivo de una sola organización que comprende varios consumidores (por ejemplo, unidades de negocios). Puede ser propiedad, administrado y operado por la organización, un tercero o alguna combinación de ellos, y puede existir dentro o fuera de las instalaciones.

- Nube pública. La infraestructura en la nube está prevista para uso abierto por el público en general. Puede ser propiedad de, administrado y operado por una organización empresarial, académica o gubernamental, o una combinación de ellos. Existe en las instalaciones del proveedor de la nube.
- Nube híbrida. La infraestructura en la nube es una composición de dos o más infraestructuras en la nube distintas (privada, comunitaria o pública) que siguen siendo entidades únicas, pero están unidas por una tecnología patentada o estandarizada que permite la portabilidad de datos y aplicaciones (por ejemplo, la explosión de la nube para el equilibrio de carga entre nubes).
- Nube comunitaria. La infraestructura en la nube se proporciona para uso exclusivo de una comunidad específica de consumidores de organizaciones que tienen inquietudes compartidas (por ejemplo, misión, requisitos de seguridad, políticas y consideraciones de cumplimiento). Puede ser de propiedad, administrada y operada por una o más de las organizaciones de la comunidad, un tercero o alguna combinación de ellas, y puede existir dentro o fuera de las instalaciones.

### 2.1.3. Problemática de la Nube

Aunque la Computación en la Nube es en gran medida considerada como el futuro de la tecnología empresarial y de los consumidores, no deja de tener sus inconvenientes y defectos que lo impiden para aquellos que tienen necesidades muy especiales en su organización.

El primer problema detectado en su aparición fue el shock en la cultura corporativa. Las organizaciones están acostumbradas a hacer todo por sí misma y tener el poder sobre todo lo que está sucediendo alrededor de ella. Con la adopción de la Computación en la Nube, su rutina de trabajo ha cambiado dramáticamente y con frecuencia se encuentra trabajando en algo que realmente no necesita más. Esto también tiene un impacto en los administradores, que acostumbrados a ser los gestores de servicio interno pasan a ser gerentes de servicios externos.

Además del shock o cambio cultural en la organización, los problemas más importantes revelados son [28]:

- Seguridad de los datos. A diferencia de los sistemas internos, la Computación en la Nube está en línea y accesible a cualquier persona que sabe cómo usarlo. De la misma forma que si los datos o servicios se hubieran proporcionado internamente, la seguridad se puede hacer más robusta ya que la conexión total desde el mundo exterior se puede cortar. Una preocupación creciente es también el intercambio de datos en Internet, que tienden a no ser seguras, ya que las líneas pueden ser inhaladas y leídas por terceros. El hecho es que no sabrás quién puede ver y manipular tus datos cuando está controlados por un proveedor externo.
- Preocupaciones de privacidad. Cuando terceros manejan tus datos, no hay ninguna garantía de que no hayan visto ninguna parte de ellos durante el mantenimiento de la infraestructura.
- Implementación insegura: Permite el acceso a la misma desde elementos remotos, puede ofrecer el acceso a nuestra nube y datos por parte de terceros no autorizados.
- Actualizaciones de seguridad: Al tratarse de entornos de 'software', es importante que los sistemas se actualicen con las últimas versiones que hayan sido validadas como correctas, para evitar ataques apoyados en posibles vulnerabilidades.
- No hay normas y leyes estándar, y sin estas las cosas poco a poco se vuelven caóticas, ya que cada proveedor puede implementar sus propios sistemas de manera muy diferente de otros proveedores, por lo que se hará más difícil para las personas el trasladarse de un proveedor a otro a causa de incompatibilidades.

En el aspecto negativo se puede destacar que los datos están fuera de la organización. Esto supone para algunos cierto temor por si el proveedor sufriera algún problema. Además en algunos casos se podría estar incurriendo en una infracción, al exigir ciertas leyes el acceso a la información. Muchos de estos servidores están en países diferentes al de la organización que accede a ellos [27].

## 2.2. Vulnerabilidades y ataques informáticos

Una vulnerabilidad es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información permitiendo que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estas debilidades o fallas pueden tener distintos orígenes, entre los que se destacan: fallos de diseño, errores de configuración, carencias de procedimientos o limitaciones propias de la tecnología [29].

### 2.2.1. Vulnerabilidades y Exposiciones Comunes

Actualmente se emplea una nomenclatura común para el conocimiento público de vulnerabilidades, con el fin de facilitar el intercambio de información entre diferentes bases de datos y herramientas. La misma se denomina Vulnerabilidades y Exposiciones Comunes, que proviene del inglés "Common Vulnerabilities and Exposures" (CVE).

CVE comprende una lista de nombres estandarizados para vulnerabilidades y otras exposiciones de seguridad de la información. Su propósito es estandarizar los nombres para todas las vulnerabilidades y exposiciones de seguridad de conocimiento público [30].

CVE es un diccionario cuyo propósito es propiciar la distribución de datos en bases de datos de vulnerabilidades y herramientas de seguridad separadas. Facilita la búsqueda de información en otras bases de datos y no se debe considerar como una base de datos de vulnerabilidades por sí sola [30].

CVE se mantiene a través de un esfuerzo de colaboración comunitario conocido como Consejo Editorial de CVE. El Consejo Editorial incluye representantes de numerosas organizaciones relacionadas con la seguridad, como proveedores de herramientas de seguridad, instituciones académicas y gobiernos, además de otros expertos en seguridad. La organización The MITRE Corporation preserva CVE y modera debates del Consejo Editorial [30].

En seguridad informática es importante trabajar con productos y servicios

compatibles con CVE. Esto significa que una herramienta, un sitio web, una base de datos o un servicio utilizan nombres CVE de una manera que permite a este sistema establecer vínculos cruzados con otros repositorios que utilizan nombres CVE. Los mismos deben cumplir con los cuatro requisitos:

- Posibilidad de búsquedas a través de CVE: Un usuario debe poder buscar vulnerabilidades e información relacionada utilizando el nombre CVE.
- Salida CVE: La información proporcionada debe incluir los nombres CVE relacionados.
- Asignación: El propietario del repositorio debe proporcionar una asignación relacionada con una versión específica de CVE y realizar un esfuerzo de buena fe para garantizar la precisión de dicha asignación.
- Documentación: En la documentación estándar de la organización se debe incluir una descripción de CVE, la compatibilidad con CVE y la información detallada sobre cómo sus clientes pueden utilizar la funcionalidad relacionada con CVE de su producto o servicio.

Los nombres CVE son identificadores exclusivos y comunes para vulnerabilidades de seguridad de la información de conocimiento público. Los nombres CVE tienen estado de "entrada" o "candidato". El estado de entrada indica que el nombre CVE se ha aceptado en la lista de CVE, mientras que el estado de candidato (también denominado "candidatos", "números de candidatos" o "CAN") indica que el nombre se encuentra en proceso de revisión para su inclusión en la lista [30].

Cada nombre CVE incluye lo siguiente:

- Número de identificador CVE (es decir, "CVE–1999–0067").
- Indicio de estado de "entrada" o "candidato".
- Breve descripción de la vulnerabilidad o exposición de seguridad.
- Cualquier referencia pertinente (es decir, informes y boletines de vulnerabilidad).

Por otra parte, las vulnerabilidades se clasifican en cuatro tipos, dependiendo de la amenaza que puede significar y la complejidad de aplicación [31]:

- Crítica: Vulnerabilidad que permite la propagación de amenazas sin que sea necesaria la participación del usuario.
- Importante: Vulnerabilidad capaz de poner en riesgo la confidencialidad, integridad o disponibilidad de los datos de los usuarios, como así también, la integridad o disponibilidad de los recursos de procesamiento que este disponga.
- Moderada: Vulnerabilidad que presenta un riesgo que se puede disminuir con medidas tales como configuraciones predeterminadas y auditorías principalmente.
- Baja: Vulnerabilidad muy difícil de aprovechar por un atacante, y su impacto es mínimo, ya que no afecta a una gran masa de usuarios.

### 2.2.2. Estadísticas de vulnerabilidades

La seguridad es uno de los principales problemas de sistemas de información basados en la Computación en la Nube. Los vectores de ataques son las vulnerabilidades y su conexión en una red de redes incrementa la exposición a ataques de hackers.

De acuerdo a lo publicado por el centro de investigación de Tenable en el "Informe de inteligencia de vulnerabilidades" [3], el descubrimiento y la revelación de vulnerabilidades continúa aumentando en términos de volumen y ritmo. Durante 2017 se publicó un promedio de 41 nuevas vulnerabilidades por día, lo que genera un total de 15.038 por año. Mientras que en 2018 se detectaron 16.955 vulnerabilidades nuevas, lo que mostró un aumento del 13% respecto a 2017 [3].

Además de la ingeniería social como el vector de ataque inicial, la mayoría de las filtraciones de datos modernas son una consecuencia directa de una gestión de vulnerabilidades ineficaz.

Las vulnerabilidades de alto perfil, se mencionan como la causa principal de la filtración masiva de datos. Muchos incidentes de alto perfil podrían haberse evitado con una mejor higiene cibernética, ya que la mayoría de las filtraciones de datos no suponen ataques sofisticados ni exploits de día cero. De hecho, 57% de las organizaciones que fueron objeto de una filtración de datos en los últimos años confirman que una vulnerabilidad conocida y sin parches fue la causa principal. Además, se destaca que el 52% de las organizaciones tienen una evaluación de vulnerabilidades de madurez baja [3].

El crecimiento interanual promedio desde 2010 ha sido del 15%, y el aumento de las vulnerabilidades reveladas y las CVE publicadas continúa sin disminuir en 2019. En el gráfico de la Figura 2, se observa el incremento de vulnerabilidades publicadas dentro de CVE desde 2010 a 2019 [3].

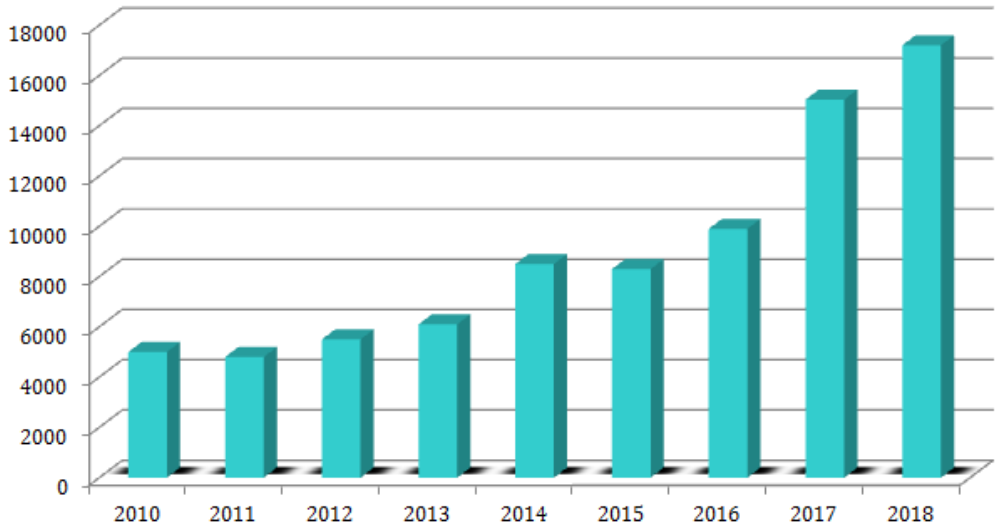



**Figura 2**. Cantidad de vulnerabilidades CVE publicadas por año.

En cuanto a las características de las vulnerabilidades, es importante tener en cuenta su criticidad como el nivel de explotación. La criticidad determina que tan grave puede ser su explotación, por lo que son categorizados en vulnerabilidad: Alta, Media, Baja e Informacional.

El nivel de explotación es otro factor crucial ya que está determinado por la cantidad e importancia de los servidores que pueden llegar a tener dicha vulnerabilidad. Si la vulnerabilidad afecta a clases servidores que predominan a nivel mundial, su clasificación se conoce como de Riesgo Global. Por otro lado, si la vulnerabilidad independientemente de

su criticidad afecta a pocos servidores, se clasifica como Riesgo Local.

Las vulnerabilidades de aplicaciones representan otro conjunto de CVE activamente blanco de los actores de amenazas que circulan libremente en diversos ataques, que van desde la ejecución por explotación y la piratería de criptomonedas hasta la suplantación de identidad (Phishing).

### 2.2.3. Ataques informáticos

Existen numerosos casos a nivel mundial de importantes y prestigiosas organizaciones que fueron víctimas de ataques informáticos, filtrados mediante vulnerabilidades en los sistemas operativos y software instalado en los equipos/servidores. Los ataques más comunes permiten la ejecución de código remoto sobre el equipo infectado, robo de datos, denegación de servicios, eliminación o modificación de ficheros y cifrado de archivos. Dentro de los ataques más relevantes registrados en la historia de la informática, tenemos dos casos puntuales que ocurrieron durante 2017 y se realizaron mediante el vector de infección EternalBlue.

EternalBlue es un exploit desarrollado por la NSA que fue filtrado por el grupo de hackers Shadow Brokers el 14 de abril de 2017, y fue utilizado en el ataque mundial de Ransomware con WannaCry el 12 de mayo de 2017 y en el ataque de Ransomware con la variante Petya el 27 de junio de 2017 [32].

EternalBlue aprovecha una vulnerabilidad en la implementación del protocolo Server Message Block (SMB) de Microsoft. Esta vulnerabilidad, denotada como CVE-2017-0144 en el catálogo Common Vulnerabilities and Exposures (CVE), se debe a que la versión 1 del servidor SMB (SMBv1) y acepta en varias versiones de Microsoft Windows paquetes específicos de atacantes remotos, permitiendo ejecutar código en el ordenador en cuestión [32].

La actualización de seguridad de Windows que lanzó Microsoft el 14 de marzo de 2017 resolvió el problema a través del parche de seguridad MS17-010, para todas las

versiones de Windows. En la fecha indicada el lanzamiento fue para todas las versiones mantenidas dentro del ciclo de vida de Microsoft, y posteriormente liberó para versiones antiguas como Windows XP y Windows Server 2003.

Por diversos motivos, muchos usuarios de Windows no habían instalado MS17-010 cuando, dos meses más tarde, el 12 de mayo de 2017, se produjo el ataque del Ransomware WannaCry que empleaba la vulnerabilidad EternalBlue [32].

Los ataques Ransomware de la variedad WannaCry son ataques informáticos que usan el criptogusano conocido como WannaCry dirigidos al sistema operativo Windows de Microsoft. Durante el ataque, los datos de la víctima son encriptados, y se solicita un rescate económico pagado con la criptomoneda Bitcoin, para permitir el acceso a los datos [33].

El ataque del viernes 12 de mayo de 2017 ha sido descrito como sin precedentes en tamaño, infectando más de 230.000 servidores en más de 150 países y generó costes totales de alrededor 4 mil millones de dólares. Los países más afectados que han sido reportados son Rusia, Ucrania, India y Taiwán, pero partes del servicio nacional de salud de Gran Bretaña (NHS), Telefónica de España, la red de ferroviaria en Alemania, organismos públicos de Rusia, universidades en China, FedEx, Deutsche Bahn, y las aerolíneas LATAM, junto con muchos otros blancos a nivel mundial [34].

En Argentina, la gravedad se explica por la vulneración simultánea de grandes organizaciones y no tanto por la cantidad de terminales afectadas, ya que solo se registraron 2500 reportes. Entre ellos, los casos más destacados se reportaron en el Gobierno de la Ciudad de Buenos Aires y en la compañía de telefonía Claro Argentina [34].

Los ataques Ransomware normalmente infectan un ordenador cuándo un usuario abre un email Phishing, utilizando técnicas de ingeniería social para convencer a estos usuarios de descargar archivos o abrir enlaces Web. En ambos casos, el virus se descarga y ejecuta localmente en el equipo, como lo muestra la Figura 3. Una vez instalado, WannaCry utiliza el exploit EternalBlue para extenderse a través de redes locales y anfitriones remotos que no hayan recibido la actualización de seguridad, y de esta manera infecta directamente cualquier sistema expuesto [33].

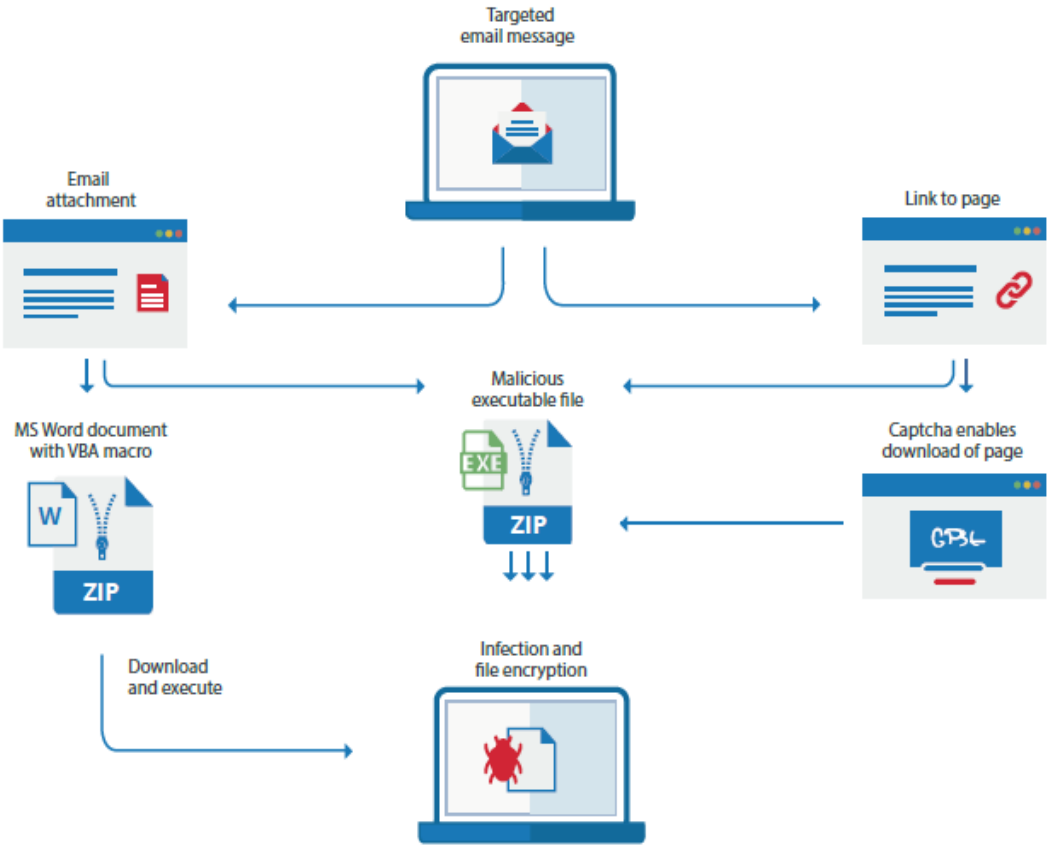



**Figura 3.** Método de ataque de Ransomware mediante correo.

En los equipos infectados, WannaCry crea claves de registro y modifica otras, crea y ejecuta procesos locales y cifra todos los documentos y archivos que encuentra, a quienes les cambia los nombres y le añade ".Wncry" al final. Además, reemplaza la imagen de fondo del escritorio por una negra con un mensaje del ataque y genera una pantalla como se muestra en Figura 4, donde se solicita un rescate para que el usuario pueda recuperar sus datos [35].


**Figura 4.** Mensaje de infección de Ransomware en equipo.

En otra instancia, un nuevo ataque se registró el martes 27 de Junio de 2017 donde un virus informático se propagó amenazando a miles de organizaciones del todo el mundo. Se destacan los sistemas del Banco Central de Ucrania, la petrolera rusa Rosneft y el aeropuerto de Boryspil entre los más afectados, al igual que varias multinacionales como la farmacéutica MSD y la compañía de alimentación Mondelez. En Argentina se registraron nuevamente miles de equipos afectados en los que se destacan organizaciones de publicidad y Ogilvy. En este caso, el virus informático es un Ransomware con la variante llamada Petya que del mismo modo que WannaCry, utiliza la vulnerabilidad en el protocolo para compartir en red (SMBv1) de los sistemas operativos Windows denominada EternalBlue, lo que permite la infección del equipo local y la propagación a otros equipos mediante las redes locales [34].

Una de las diferencias funcionales que presentan estas dos variantes de Ransomware, es que Petya en lugar de cifrar los ficheros uno a uno como WannaCry, reinicia el equipo de la víctima y cifra la tabla maestra de archivos del disco duro y hace que la partición encargada de arrancar el sistema quede inutilizable al reemplazarlo con un código que muestra aviso

de rescate.

El parche crítico MS17-010 había sido emitido por Microsoft el 14 de marzo de 2017 para eliminar la vulnerabilidad subyacente, lo cual se dio casi dos meses antes del primer ataque y tres meses del segundo, sin embargo, muchas organizaciones no las aplicaron.

De manera similar y tiempo después, siguieron los ataques informáticos a nivel mundial, aprovechando vulnerabilidades de seguridad generadas por la no aplicación de actualizaciones existentes. Durante 2018 se destaca el ciberataque en los Juegos Olímpicos de Invierno de Pieonchang, donde al momento de la ceremonia de inauguración, atacantes pudieron interferir con la conexión de Internet, el sitio Web y los servicios de televisión. Este virus informático es un Ransomware con la variante llamada Bad Rabbit mediante el vector de ataque denominado EternalRomance, que también utiliza SMB y permite la infección del equipo local y la propagación a otros equipos mediante las redes locales. Otros casos similares ocurrieron principalmente con las variantes: AdyLkuzz, NotPetya y PyRoMine, que utilizan los vectores EternalBlue y EternalRomance amenazando sistemas sin parches [34].

Durante el año 2018 también se destacó el ataque perpetrado por el grupo de hackers chino apodado Red Apollo, quién lanzó una de las campañas mundiales de espionaje cibernético más grandes de la historia [5]. En lugar de atacar directamente a compañías, se dirigió a proveedores de servicios en la nube y aprovechando vulnerabilidades en sus sistemas operativos, infectó los servidores y usó sus redes para difundir herramientas de espionaje a un gran número de organizaciones. El objetivo del ataque, llamado Operación Cloud Hopper, era un pequeño número de proveedores de servicios informáticos, por lo que podía propagar malware a todos los clientes que utilizaban estas plataformas para gestionar sus redes informáticas. Como resultado de este ataque, se vieron afectadas organizaciones de quince países, entre ellos Reino Unido, Francia, Suiza, Estados Unidos, Canadá, Australia y Japón [5].

Los ataques de malware y Ransomware son las consecuencias más llamativas de una vulnerabilidad sin parchear, pero no las únicas. Durante 2018 y 2019, comenzaron a ocurrir ataques asociados a la minería de monedas digitales o criptomonedas y los casos Spectre and

Meltdown.

Spectre y Meltdown son dos vulnerabilidades que se generaron debido a un error de diseño en los microprocesadores que afecta a los fabricantes Intel, AMD y ARM. Esta vulnerabilidad permite a un software malicioso espiar lo que están haciendo otros procesos y también espiar los datos que están en esa memoria en el ordenador atacado. En otras palabras, podrían permitir que un atacante capture información de chips a las que no deberían poder acceder, incluidas contraseñas y claves [36].

En cuanto a las criptomonedas, es popularmente conocido que el mercado de monedas digitales está creciendo. Esto requiere que existan más mineros, es decir, aquellas personas que cuentan con la actividad computacional necesaria para procesar las transacciones que se realizan con estas divisas. Los mineros se encargan de usar el procesamiento de sus ordenadores, los cuales pueden ser comunes o especializados para esta tarea, y a cambio reciben una compensación económica en esa misma divisa digital, la cual puede canjearse por dólares o euros [37].

Aunque la minería de las también llamadas criptomonedas es legal, se ha encontrado que los cibercriminales están creando diversas campañas para aprovecharse de esto y ganar dinero fácil. Es el caso del Cryptojacking, en el que los hackers inyectan código en sitios Web que de otro modo serían legítimos, obligando a sus visitantes a extraer criptomonedas utilizando sus propios recursos de hardware durante su permanencia. Si bien este tipo de ataque puede parecer más "sano" que sus predecesores, ya que los piratas informáticos no roban nada más que el poder de cómputo, lo cierto es que los dispositivos sufren una degradación más rápida [38].

Conforme los mercados de criptomonedas crezcan, hay más sentido para que los cibercriminales se dediquen a la minería. Es mucho menos riesgoso para ellos, tienen utilidades altas y no son perseguidos por las autoridades. Si bien existen varios métodos por el cual los atacantes pueden hacerse del procesamiento del equipo, los más importantes están centrados en vulnerabilidades de aplicaciones Web, como es el caso de navegadores no actualizados o parcheados [37].

## 2.3. Soluciones y modelos existentes

Los fabricantes y desarrolladores de software mensualmente publican boletines de seguridad con parches para hacer frente a las fallas y debilidades de sus productos. Estos boletines contienen un conjunto de parches de seguridad que corrigen vulnerabilidades de seguridad en software, se describen las soluciones y se proporcionan vínculos a las actualizaciones correspondientes del software afectado. Cada boletín va acompañado de un artículo de Knowledge Base exclusivo en el que se proporciona más información sobre las actualizaciones.

### 2.3.1. Parches y actualizaciones

Un parche es una acumulación de correcciones para un posible problema o problema conocido del sistema operativo u otro software. También puede proporcionar una nueva función, una mejora a una determinada versión de software o corregir una vulnerabilidad existente. Un parche consta de archivos y directorios que sustituyen o actualizan archivos y directorios existentes. Por lo tanto, los parches se utilizan para los siguientes fines [39]:

- Proporcionar soluciones de vulnerabilidades.
- Proporcionar correcciones de errores.
- Proporcionar nuevas funcionalidades.
- Proporcionar nuevo soporte de hardware.
- Proporcionar mejoras de rendimiento y mejoras para las utilidades existentes.

Los parches se identifican mediante identificadores de parche únicos. Un ID de parche es una cadena alfanumérica que es un código base de parche y un número que representa el número de revisión del parche unidos por un guión [39]. Los parches que solucionan vulnerabilidades están asociados directamente a identificadores de vulnerabilidades CVE.

Las actualizaciones que presentan los productos o soluciones de software, concentran sus beneficios en las nuevas funcionalidades que presentan, pero también contienen correcciones de errores y parches de vulnerabilidades detectadas.

Las actualizaciones, ya sean de seguridad o de funcionalidad, de los sistemas deben estar guiadas por un proceso de gestión de parches que identifique adecuadamente el ciclo de vida e indique su periodicidad [40].

Una estrategia efectiva de gestión de parches es fundamental para distribuir actualizaciones de software y, lo que es más importante, para detectar y reparar las vulnerabilidades de seguridad. Muchos ataques exitosos se cometen contra las vulnerabilidades previamente conocidas para las que el proveedor de software ya disponía de una revisión o estándar de configuración segura. Sin embargo, estas parches únicamente son efectivas si se han implementado [41].

La gestión de parches implica aplicar parches y actualizaciones de software a un sistema. Es posible que la gestión de parches también implique eliminar parches no deseados o defectuosos [39].

### 2.3.2. Buenas prácticas de seguridad

Microsoft Security Response Center publica boletines de seguridad cada mes para describir las actualización de seguridad que se publican dicho mes. Planifican su publicación el segundo martes de cada mes aunque es posible que realicen alguna publicación fuera de esta fecha, en caso de que el boletín sea de carácter urgente.

Del mismo modo que lo hace Microsoft, todos los fabricantes de software publican parches y actualizaciones de sus productos con mejoras funcionales, corrección de fallas y vulnerabilidades. Dependiendo de los casos, se detectan publicaciones desde semanales a anuales. En el caso de Microsoft se destaca que es la única organización mundial de software con una fecha fija de publicación; y además, que sus productos abarcan el mayor porcentaje de usuarios en el mundo.

Se considera una buena práctica de seguridad revisar e instalar los parches que los boletines proponen en el mismo momento en que son publicadas. Ésto es debido a que al instante de su publicación, las vulnerabilidades se hacen públicas y los atacantes astutos pueden aprovecharlas para realizar algún tipo de acción maliciosa.

Los principales motivos que se observan en base a la no aplicación de actualizaciones de seguridad en las organizaciones son los siguientes [42]:

- No brindan disponibilidad de recursos humanos a cuestiones generales de seguridad informática.
- No utilizan herramientas centralizadas de gestión de actualizaciones de seguridad.
- Utilizan herramientas de gestión de actualizaciones pero no analizan en profundidad los servidores y escritorios.
- Aplican solo actualizaciones de seguridad generales recomendadas por Windows Update sin realizar un escaneo profundo.
- Analizan completamente los servidores y equipos, y se liberan todas las actualizaciones requeridas pero los administradores de éstos no aplican las actualizaciones con regularidad.
- Por cuestiones de disponibilidad 7x24 de los servicios, los administradores no reinician los servidores para finalizar el proceso de actualización.
- No disponen de un proceso completo con herramientas de seguridad que le permitan detectar vulnerabilidades y debilidades a nivel de software, para mitigarlas o eliminarlas.

Para dar respuesta al problema de mantener actualizados los servidores en Nube privada en las organizaciones, existen múltiples modelos existentes como así también herramientas de seguridad específicas.

### 2.3.3. Soluciones y modelos existentes

Actualmente existen distintas soluciones de seguridad que ofrecen un sistema de

gestión de vulnerabilidades aunque presentan limitaciones importantes. A continuación se describen las soluciones destacadas y sus limitantes:

- Microsoft fue la primera compañía internacional que desarrolló una solución que presenta detección de vulnerabilidades existentes, liberación e instalación de actualizaciones [12], pero es una solución incompleta ya que el analizador de vulnerabilidades solo detecta nuevas versiones disponibles de Software a las cuales recomienda actualizar y no presenta un listado de vulnerabilidades completo. Además, sólo es aplicable a software de Microsoft.
- Akamai es un fabricante de soluciones de seguridad que ofrece una herramienta de distribución de actualización, parches y aplicaciones a los usuarios con una experiencia de descarga rápida, segura y excepcional, optimiza las descargas, entregas e instalación, simplificando la gestión [13]. Si bien es una solución potente aplicable a todo tipos de sistemas operativos y aplicaciones, no permiten el ajuste a una política de seguridad organizacional, no presenta buenas prácticas de seguridad, no se adapta a ningún estándar de seguridad internacional y no ofrecen modelos de madurez.
- Kace es una solución de seguridad que se destaca por su capacidad de automatizar la administración e implementación de parches, a partir de una de las bibliotecas de parches más grandes de la industria. Incluye parches para sistemas operativos Windows y Mac, y para todas las aplicaciones oficiales. Permite realizar auditorías de seguridad, identificar vulnerabilidades y ajustar a políticas de seguridad [14]. A pesar de sus bondades, es una solución incompleta ya que no está alineado a estándares de seguridad, no ofrece cumplimientos de buenas prácticas de seguridad, no disponen de mecanismo de monitoreo y no ofrecen modelos de madurez.

Por otro lado, se detectan distintos trabajos de investigación relacionados con la seguridad en servidores y en la computación en la nube, aunque presentan restricciones importantes sobre su modelo de seguridad:

- La propuesta de Jouini & Rabai (2019) titulada "A security framework for secure cloud computing environments. In Cloud Security: Concepts, Methodologies, Tools, and Applications" [15] describe las capacidades de la tecnología de computación en la nube como así también los obstáculos de seguridad a los cuales se debe enfrentar.

  En este documento, los autores tratan los problemas de seguridad en los sistemas de computación en la nube y hacen su aporte desarrollando un modelo de seguridad basado en evaluación de riesgos cuantitativos.

  Las principales limitantes de su propuesta se centran en que no se alinea a algún estándar de seguridad y no visualizan la importancia de la gestión de vulnerabilidades.

- La propuesta de Rittinghouse & Ransome (2016) titulada "Cloud computing: implementation, management, and security" [16] proporciona una comprensión de lo que significa la computación en la nube, explora qué tan disruptivo puede llegar a ser en el futuro, analiza las amenazas de seguridad y examina sus ventajas y desventajas. Como aporte, proporciona a los ejecutivos de negocios el conocimiento necesario para tomar decisiones informadas y educadas con respecto a las iniciativas de la nube, brindando buenas prácticas de seguridad.

  La falencia de esta propuesta se basa en que las recomendaciones son generales, no se ajustan a estándares de seguridad y tampoco hace hincapié en la importancia de la gestión de vulnerabilidades.

- El diseño de Haber & Hibbert (2018) titulado "Vulnerability Management Design. In Asset Attack Vectors" [17] describe la importancia de reducir los riesgos de un ataque cibernético al encontrar y cerrar agujeros en la infraestructura de TI, para lo cual propone un programa de administración de vulnerabilidad. Este programa se diseñó con el objetivo de garantizar que las personas, los procesos, las políticas y las tecnologías seleccionadas trabajen juntas para proteger y defender proactivamente a las organizaciones de las amenazas informáticas.

Si bien este diseño refiere a la gestión de vulnerabilidades como el tema de mayor importancia para la seguridad, no se alinea a un estándar de seguridad internacional, y la política y los procesos propuestos son generalistas.

- El framework de Poonia, Banerjee, Banerjee, & Sharma (2018) titulado "Vulnerability identification and misuse case classification framework" [18] describe la especificación de la seguridad como un requisito no funcional y la dificultad en lo que respecta a su identificación e implementación. Además, detecta la gran cantidad de métodos y técnicas para la implementación de la seguridad durante el desarrollo de la aplicación de software, como así también las falencias existentes en cuanto a la identificación de vulnerabilidades y su tratamiento adecuado, sobre todo, teniendo en cuenta la preocupación por la alineación de los objetivos comerciales y sus activos asociados y el riesgo relacionado con las vulnerabilidades identificadas. Para esto propone un marco para la identificación de vulnerabilidades adecuadamente alineadas con los objetivos comerciales y los activos asociados y su riesgo de la aplicación de software en desarrollo. Para evaluar estas vulnerabilidades, presenta una clasificación ontológica del caso de uso indebido a través de un modelo de sistema.
  Si bien es un modelo de seguridad completo, no se adapta a tecnologías de Computación en la Nube, los estándares a los cuales se alinean no son de seguridad de la información y no define un proceso operacional claro.

- El modelo de Krutz & Vines (2010) que presentaron en el artículo "Cloud security: A comprehensive guide to secure cloud computing" [19] es un modelo completo de seguridad que define procesos de gestión y operación. Describen principalmente fundamentos de la Computación en la Nube, arquitectura, fundamentos de seguridad, riesgos de computación en la Nube y desafíos de seguridad. Además, proponen una arquitectura de seguridad y ciclo de vida de la informática en la Nube.
  A pesar de su visión completa de la problemática de seguridad en la Computación en la Nube, actualmente es un modelo que no es posible

implementar ya que quedó obsoleto. Está definido en base a los primeros conceptos de Computación en la Nube y con los cambios tecnológicos que ocurrieron en los últimos años, no contempla las arquitecturas de Nube actuales ni las amenazas de seguridad avanzadas.

### 2.3.4. Herramientas de seguridad

El Estándar ISO/IEC 27000 dentro del control "12.6 Control de las vulnerabilidades técnicas" establece: "Se debería obtener información oportuna sobre la vulnerabilidad técnica de los sistemas de información que se están utilizando, evaluar la exposición de la organización ante tal vulnerabilidad y tomar las medidas adecuadas para hacer frente a los riesgos asociados" [42]. Uno de los elementos principales para lograr esta premisa, se basa en el uso de herramientas de seguridad que permitan optimizar y automatizar las tareas.

La variedad de herramientas de Software para realizar el escaneo y explotación de vulnerabilidades es amplia, y es cuestión de elegir cuál es la herramienta que mejor se adapte a las necesidades de la infraestructura de la organización, o a la exigencia de la prueba a ejecutar [43].

En toda organización con sistemas de información, hay una serie de amenazas potenciales: errores de configuración, errores humanos, políticas de seguridad pobres y otras vulnerabilidades que pueden ser explotadas por un atacante. Para contrarrestar todas las vulnerabilidades, las organizaciones deben trabajar con herramientas informáticas que permitan realizar análisis de vulnerabilidades, pruebas de penetración, distribución de parches y actualizaciones, y configuraciones de seguridad [44].

Inicialmente las organizaciones deben realizar análisis de vulnerabilidades de manera regular. Como requerimiento, quienes trabajan en seguridad de la información necesitan permiso de su organización para probar las redes en vivo y necesitan las herramientas de pruebas de penetración adecuadas para el trabajo [44].

Existen múltiples herramientas de penetración y análisis de vulnerabilidades, algunas

son gratuitas y otras no, pero todas sirven un propósito: encontrar las vulnerabilidades antes de que los hackers lo hagan. No hay dos herramientas que tengan las mismas técnicas de penetración. Cada herramienta se diferencia en sus métodos de exploración así como en los tipos de vulnerabilidades que buscan. Algunas son específicas para los sistemas operativos, y otras son agnósticas [44].

Las herramientas mayormente recomendadas dentro del entorno de la seguridad de la información son:

- Microsoft Baseline Security Analyzer - Microsoft Corporation: MBSA es un analizador de seguridad de base de Microsoft. Es una de las aplicaciones que ofrece Microsoft para verificar la seguridad de los equipos que emplean su sistema operativo Windows. Esta utilidad permite verificar la seguridad de la máquina, o la de un conjunto de ellas dentro de la red, ofreciendo información acerca del estado de los puertos abiertos en la conexión TCP/IP, los parches de seguridad instalados y toda una serie de vulnerabilidades a las que se pueden ser susceptibles, incluso las que afectan al propio navegador web. Además, suministra información y recomendaciones que permitirán resolver las incidencias, blindando más las máquinas y los datos que contienen [45].

- Nessus - Tenable Network Security: Es un escáner de seguridad remoto multiplataforma que está basado en plugins, permite generar reportes y sugiere soluciones para los problemas de seguridad. Es capaz de identificar las vulnerabilidades, configuraciones de violar la política y malware que los atacantes podrían utilizar para penetrar en su red. Dispone de amplia biblioteca de comprobación de vulnerabilidad de la industria y soporta una gran variedad de tecnologías [46].

- Otras herramientas similares: Nexpose, Nipper, OpenVAS, QualysGuard, Retina, SAINT, Zenmap y Burp. Si bien Nessus y MBSA son las más populares y utilizadas, estas son otras herramientas recomendadas para análisis de vulnerabilidades y pruebas de penetración [43][44].

También es aconsejable realizar escaneos sobre aplicaciones Web o portales publicados en servidores en Nube "as a services". Tienen la ventaja de ser capaces de detectar vulnerabilidades en los servidores como así también en las aplicaciones en sí mismas. Es útil para escanear servicios publicados en Nube, donde no se tiene control sobre la infraestructura. Dentro de las herramientas disponibles, se destaca la siguiente:

- Acunetix Web Vulnerability Scanner: Acunetix es una herramienta capaz de escanear sitios web en busca de posibles fallos de seguridad que puedan poner en peligro la integridad de la página publicada en Internet. Esta aplicación ejecuta una serie de pruebas, totalmente configurables por el usuario, para identificar las vulnerabilidades tanto en la programación de la página como en la configuración del servidor.

Posterior a la detección de vulnerabilidades asociadas a los servidores y sus correspondientes actualizaciones o parches a instalar, es necesario distribuir los mismos para ser instalados. Si se tiene en cuenta la numerosa cantidad de activos que puede llegar a tener una organización, la actualización de los mismos de manera manual podría llegar a ser imposible.

Es necesaria una herramienta automatizada que permita la distribución de parches y actualizaciones de manera centralizada, que permita obtener y entregar los parches a los servidores, instalándolos localmente.

La herramienta mundialmente utilizada para esto es conocida como WSUS pero se aplica sólo a componentes de Microsoft. De todos modos, existen múltiples herramientas y para diferentes plataformas, entre las que se destacan:

- Windows Server Update Services – Microsoft Corporation: WSUS es una herramienta informática que permite a los administradores de las tecnologías de la información implementar las actualizaciones más recientes de los productos de Microsoft en los equipos con sistemas operativos Windows. Mediante WSUS, los administradores pueden gestionar completamente la distribución de las actualizaciones lanzadas al mercado a través de Microsoft Update a los equipos de la

red, de manera centralizada [47].

- CFEngine: Sistema de gestión de configuración multiplataforma de código abierto. Su función principal es proporcionar la configuración y el mantenimiento automatizados de los sistemas informáticos a gran escala, incluida la administración unificada de servidores, equipos de escritorio, dispositivos industriales y de consumo, dispositivos integrados en red, teléfonos inteligentes móviles y tabletas [48].

Es importante tener en cuenta que desde el momento de que una vulnerabilidad es publicada, hasta que es instalado el parche que corrige dicha vulnerabilidad, existe un lapso de tiempo considerable donde el activo está expuesto. Es casi imposible que los equipos de TI puedan mantenerse al día con la descarga, prueba e implementación de parches para todas las vulnerabilidades críticas antes de que sean explotadas [49].

El parcheo virtual protege servicios y aplicaciones ante amenazas en el momento adecuado. Trabaja desde la capa de seguridad, analizando tráfico e interceptando ataques en tránsito, de forma tal que tráfico malicioso no podrá alcanzar las aplicaciones y sistemas operativos [49]. El parcheo virtual permite recibir la protección de parches de actualización sin tener que realizar su instalación y en un tiempo mucho menor al que un fabricante puede generar una entrega, además sin tener que interrumpir la operación normal de los servicios de la organización [49].

# 3. Estándares y Marco de trabajo

## 3.1. Estándares de Seguridad de la Información

Los estándares son documentos técnico-legales que contienen especificaciones técnicas de aplicación voluntaria, aprobados por un organismo nacional, regional o internacional de normalización reconocido. Son elaborados por consenso de las partes interesadas: fabricantes, administraciones, usuarios y consumidores, centros de investigación y laboratorios, asociaciones, agentes sociales, entre otros, basados en los

resultados de la experiencia y el desarrollo tecnológico [50].

Los estándares permiten implantar de forma clara y precisa métodos y formas de trabajo concretos, que siguen un procedimiento definido. Con esto, las organizaciones que lo implementan pueden obtener ventajas competitivas ya que mejora la eficiencia y aumenta el potencial organizacional, previene errores humanos y puede derivar en ahorros económicos [50]. Además, con la certificación del estándar, la organización demuestra que cumple con todos los requisitos impuestos por la entidad certificadora.

Los estándares de seguridad de la información, en particular, aportan los siguientes beneficios: uso de mejores prácticas en materia de seguridad, contribución a la madurez de los procesos organizacionales, conjunción de distintos enfoques con un objetivo común, desarrollo y aplicación de experiencia acumulada, y creación de un marco de trabajo [50]. Dentro de los estándares de seguridad de la información más reconocidos e importantes a nivel mundial se destacan ISO/IEC 27000 y O-ISM3.

### 3.1.1. ISO/IEC 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña [9].

Esta es una serie compuesta por distintas normas que tienen por objetivo proporcionar a cualquier organización un conjunto de buenas prácticas para la gestión de la seguridad de su información, e indica el modo de implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO/IEC 27001 como forma de salvaguardar la red de información que contiene [9].

ISO/IEC 27000 es de carácter internacional, aplicable a todo tipo de organizaciones y entidades, y en un mundo que cada vez posee mayor cantidad de amenazas a nivel informático, se está convirtiendo en imprescindible para la seguridad de las organizaciones

[51].

ISO/IEC 27000 considera que las intrusiones y los ataques informáticos provienen principalmente a partir de las vulnerabilidades que presentan los servidores en sus versiones de sistema operativo, software instalado, service pack de aplicaciones, entre otros. Manteniendo los objetivos de confidencialidad, integridad y disponibilidad de la información y los sistemas dentro de la organización, es necesario identificar, analizar y prevenir las amenazas gestionando y controlando la implementación de los parches y actualizaciones correspondientes.

La norma ISO/IEC 27002 define un conjunto de buenas prácticas para aplicar en este ambiente y se identifican dentro del dominio "12. Seguridad en la Operativa" y el objetivo de control "12.6 Gestión de la vulnerabilidad técnica".

### 3.1.2. O-ISM3

El modelo O-ISM3 es un estándar de madurez de seguridad de la información orientado a procesos, adaptable a cualquier tipo de organización y compatible con la implantación de ISO/IEC 27001 [52]. El uso del estándar permite que las organizaciones puedan focalizarse sobre la adecuada administración de políticas, procesos, métricas y controles de seguridad para mitigar los riesgos sobre sus activos de información.

El Estándar O-ISM3 se basa en los procesos comunes de seguridad de la información que deberían estar implementados y gestionados. Además, se caracteriza por proporcionar un enfoque por niveles (genérico, estratégico, táctico y operacional), donde en cada nivel se implementan diferentes procesos de seguridad, los cuales pueden ir interrelacionados con procesos de otros niveles [52].

El enfoque operacional, reporta al Gerente de TI y al Gerente de Seguridad de la información, y hace hincapié en la gestión de vulnerabilidades y protección de los activos de la organización. Este enfoque se divide en 28 procesos operacionales, en el que se destaca el proceso de gestión operacional OSP-05 Actualizaciones de Seguridad, ya que es el proceso operacional de mayor importancia para reducir o mitigar amenazas asociadas a ataques o

incidentes de seguridad. Además, describe la actualización de servicios tendientes a prevenir incidentes relacionados con vulnerabilidades conocidas y mejorando de este modo la confiabilidad de los sistemas actualizados [52].

El Estándar ISO/IEC 27001 es una normativa certificable de carácter internacional, pero en sus requerimientos plantea sólo un marco de actuación y no define una guía de estricto seguimiento para la protección de servidores Web. A su vez, el modelo de seguridad que plantea el Estándar O-ISM3 propone procesos de seguridad de acuerdo a niveles pero no tiene suficiente nivel de detalle en cuanto a la ejecución de tareas operativas, documentación a generar, roles de usuarios a asignar y métricas a evaluar.

## 3.2. Marco de trabajo de Seguridad de la Información

En el artículo correspondiente al trabajo "Marco de trabajo estructurado para la seguridad de la información en servidores basado en estándares internacionales"[20] se presenta un marco de trabajo estructurado para la seguridad de la información en servidores, el cual ofrece una solución con el suficiente nivel de detalle para que pueda ser implementado en una organización. Este marco, se define bajo los requisitos y cumplimientos del Estándar ISO/IEC 27000 para la certificación de ISO/IEC 27001, y está basado en las buenas prácticas que se especifican en el modelo de seguridad propuesto por el Estándar O-ISM3, con lo cual hereda los beneficios de ambos estándares.

El marco de trabajo estructurado sienta las bases para que las organizaciones que lo implementan, trabajen bajo el esquema de cuatro módulos particulares representados en la Figura 5:

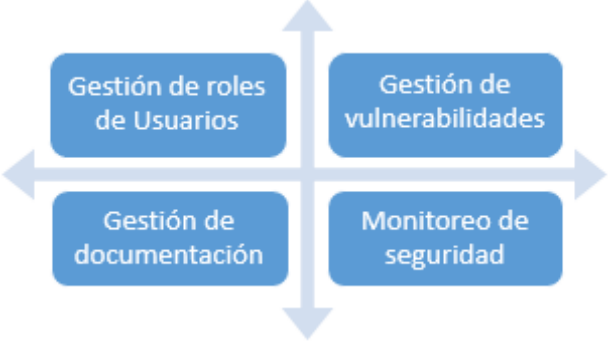


**Figura 5.** Módulos del marco de trabajo.

- Gestión de roles de usuarios con privilegios específicos, para la ejecución de tareas y acceso a documentación.
- Gestión de documentación, en el cual se propone una estructura para el almacenamiento de documentación, tanto a nivel de repositorio como de estructura de los documentos en sí mismo.
- Gestión de vulnerabilidades en una organización, mediante la implementación de un ciclo de vida o procedimiento paso a paso con las tareas que deben realizar los operadores.
- Monitoreo de seguridad de información, el cual se basa en métrica para medir el desempeño de las operaciones realizadas.

### 3.2.1. Gestión de roles de usuarios

El módulo de Gestión de roles de usuarios define cuatro roles específicos. Cada uno de estos tiene asociados un conjunto de tareas que los usuarios pueden ejecutar en base a sus permisos y responsabilidades dentro del marco de trabajo. Los roles propuestos son:

- Responsable: Usuario que define políticas, procedimientos y métricas del marco de trabajo a implementar.
- Operador: Usuario que realiza las tareas operativas sobre las herramientas de seguridad específicas en función del cumplimiento del marco de trabajo.
- Supervisor: Usuario que audita el cumplimiento de políticas y procedimientos establecidos, como así también, la consecución de las métricas definidas.
- Interesados: Usuario que por su tarea en la organización, requiere observar los resultados obtenidos del proceso.

### 3.2.2. Gestión de documentación

La propuesta de marco de trabajo estructurado presenta un módulo de gestión de

documentación donde se detalla un repositorio de documentación con la estructura de directorios del mismo, nomenclatura de nombre de archivos y formatos, principalmente, donde se almacenarán los documentos necesarios para el registro de la operación del marco de trabajo. Este módulo surge del requerimiento que impone el Estándar ISO/IEC 27002 en el dominio "12 Seguridad en la Operativa" asociado a definir y controlar una estructura de documentos actualizados, y a partir de la propuesta del Estándar O-ISM3 que especifica requerimientos de documentación y repositorios de almacenamiento.

El repositorio propuesto presenta un conjunto de directorios específicos, donde en cada uno se almacenarán documentos puntuales con formato estandarizado. Entre ellos se destacan documentación asociada a: bibliografía, política de seguridad, proceso de trabajo, procedimiento operativo, bitácoras de acciones y reportes de resultados. Además, se propone la definición de permisos de acceso a los usuarios en cuanto a lectura o escritura de los documentos almacenados en el repositorio, dependiendo de los roles de usuarios.

Lo que destaca la Gestión de documentación propuesta, es la importancia de se cumpla que los documentos de políticas y procedimientos, como así también todas las planillas de completado periódico, presenten la misma estructura de documentación. Es decir, que la información esté ordenada del mismo modo permite que los usuarios se sientan identificados con la bibliografía y encuentren de manera más rápida la información. Esto incluye utilizar el mismo formato, color y tipografía para todos los documentos, donde se identifiquen: título, subtítulos y cuerpo de texto.

### 3.2.3. Gestión de Vulnerabilidades

El módulo de Gestión de Vulnerabilidades presenta un ciclo de vida en la gestión de parches y actualizaciones para servidores, basado en los fundamentos del proceso operacional “OSP-05 Actualizaciones de Seguridad” que propone el Estándar O-ISM3. Este ciclo de vida tiene la capacidad de controlar las actualizaciones de los sistemas y aplicativos, a fin de prevenir incidentes y/o la explotación de vulnerabilidades, y cumple con los objetivos de control especificados en el punto "12.6 Gestión de la vulnerabilidad técnica",

requeridos por el Estándar ISO/IEC_27002.

Este ciclo de vida de gestión de vulnerabilidades engloba todas las tareas operativas que se deben desarrollar para el cumplimiento del objetivo asociado a detectar y mitigar las vulnerabilidades en los servidores. Las tareas deben ser dirigidas por un usuario con el rol "Responsable", ejecutadas por uno o múltiples usuarios con rol "Operador" y auditadas por un usuario con rol "Supervisor".

El ciclo de vida propuesto consta de 6 fases, como se observa en la Figura 6:

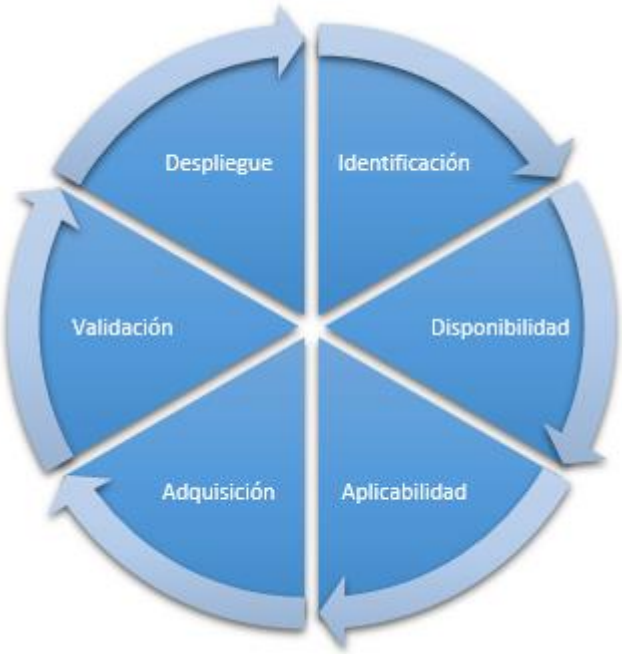



**Figura 6.** Ciclo de vida de la gestión de vulnerabilidades.

1. Identificación: En esta fase se identifican los activos y su software base instalado, así como el nivel de parches. El primer paso es contar con un inventario de activos actualizados y completos, donde se detallen todos los servidores con cada una de las aplicaciones y software instalados.
2. Disponibilidad: En esta fase se verifica la existencia y disponibilidad de parches para la mitigación de vulnerabilidades. En función del inventario de servidores y el software identificado, se ha de revisar el listado de parches detectados e identificar cuál de ellos afecta a cada activo. En la realización de

esta fase, los operadores deben trabajar con herramientas de análisis de vulnerabilidades específicas que permitan detectar posibles parches de seguridad para que solucionen las vulnerabilidades del sistema inventariado.

3. Aplicabilidad: En esta fase se valida la posibilidad real de aplicar los parches detectados y disponibles. Los parches publicados no siempre son válidos para todos los dispositivos, por lo que se ha de verificar si la actualización en concreto es apta para los activos de nuestro proceso.
4. Adquisición: En esta fase se adquieren los parches para la mitigación de las vulnerabilidades detectadas. Obtener los parches de actualización de una fuente fidedigna, comprobando la veracidad de los mismos. Para esto, se deben reconocer los sitios o fuentes oficiales de descarga de cada uno de los parches o actualizaciones, dependiendo su fabricante.
5. Validación: Durante la fase de validación se asegura que la actualización no impacta en la gestión de vulnerabilidades de forma adversa, afectando por incompatibilidad con otro componente de software o introduciendo errores. Para llevarla a cabo se han de utilizar servidores de pruebas y seguir la fase de despliegue.
6. Despliegue: La última fase del ciclo de vida se centra en distribuir las actualizaciones mediante un gestor centralizado que garantice su instalación en todos los activos requeridos.

El ciclo de vida planteado se ejecuta sobre los servidores existentes, que son detectados en la primera fase del mismo. Estos servidores se caracterizan por estar en entorno "productivo" ya que brindan servicios, por lo que son identificados desde el momento de su creación y configuración. El ciclo de vida se ejecuta de forma continua hasta el momento que, por algún motivo en particular, el servidor es quitado del área "productiva" y deja de brindar servicios.

### 3.2.4. Monitoreo de seguridad

Como parte del marco de trabajo estructurado se propone llevar a cabo el Monitoreo

de la seguridad de la información en servidores que será ejecutado por el rol de usuario "Supervisor". Es el encargado de revisar los procedimientos definidos, políticas establecidas, correcta conformación de la documentación y cumplimiento de las tareas de los demás usuarios. Además, en base a su revisión, se deben calcular y completar métricas de desempeño.

Este módulo de monitoreo responde a lo solicitado por el Estándar O-ISM3, que requiere la definición de un conjunto de métricas que permitan medir el desempeño de las operaciones realizadas. A partir de este estándar se proponen tres tipos de métricas: Métricas de implementación (IM), Métricas de eficacia y eficiencia (EF) y Métricas de impacto en el negocio (NE).

Las métricas presentadas en este módulo representan un marco de referencia. Cada organización que implementa el marco de trabajo puede agregar nuevas métricas para monitorear la seguridad de sus servidores de acuerdo a los requerimientos de negocio o técnicos de la misma.

## 3.3. Recomendaciones de seguridad

Se considera una buena práctica de seguridad revisar e instalar las actualizaciones y parches que los boletines proponen en el mismo momento en que son publicadas. Esto es debido a que desde este momento, las vulnerabilidades se hacen públicas y los atacantes astutos pueden aprovecharlas para realizar algún tipo de acción maliciosa.

Cabe destacar que, si bien es necesario y se considera una buena práctica la instalación de las actualizaciones y los parches publicados, esta tarea no se debe realizar sin antes un análisis previo. Dicho análisis debe ser exhaustivo en cada servidor, donde se debe inspeccionar cada uno de los componentes que presenta, los servicios que brinda y las hipotéticas falencias que contiene. Por este motivo, se recomienda la utilización de herramientas de escaneo de servidores, que realizan análisis de vulnerabilidades de los mismo comprobando debilidades y puntos críticos.

Posterior al análisis exhaustivo y obtención de todos los parches y actualizaciones requeridas por los servidores, surge el inconveniente del proceso de implementación de las mismas. Teniendo en cuenta que las organizaciones disponen de una gran cantidad de servidores, la gestión de sus parches se puede volver ineficiente. Los administradores de los mismos deben realizar la inspección, descargar las actualizaciones, instalarlas y finalizar el proceso dando reinicio del equipo. Además, es importante destacar que si bien cada servidor puede tener características diferentes en cuanto a servicios y funcionamiento con respecto a otro, también es cierto que presentan cuestiones en común, como parches de sistema operativo, actualizaciones o cuestiones más específicas.

La eficiencia requerida se obtiene con una herramienta informática que permite a los administradores de las tecnologías de la información implementar las actualizaciones más recientes de manera centralizada, gestionando completamente la distribución de las actualizaciones lanzadas.

Otra cuestión a tener en cuenta es la versión del software instalado y su posibilidad de obsolescencia. La herramienta de escaneo de servidores permite identificar vulnerabilidades generadas por productos de software instalados, como así también, recomendar la instalación de la última versión disponible. Si bien estas falencias son presentadas en los boletines de seguridad, no pueden ser reparadas por los parches de seguridad. Por este motivo, se establece como buena práctica analizar y actualizar la versión de software instalados en los servidores.

Si bien la actualización de parches de seguridad como así también la actualización de componentes de software es requerida para cumplir con las buenas prácticas y evitar ataques, siempre está la posibilidad de recibir ataques dirigidos que vulneren los mecanismos de seguridad establecidos, sobre todo en la ventana de tiempo que existe desde la publicación hasta la correcta instalación de cada parche. Esta ventana de tiempo, muchas veces se hace muy grande, teniendo en cuenta la imposibilidad que se presenta de reiniciar un servidor para completar la instalación debido a la criticidad de las funciones y servicios que brinda. Por este motivo, se resalta la importancia de un procedimiento de gestión de vulnerabilidades que permita optimizar las tareas y reducir los tiempos de exposición.

Un proceso completo y eficiente de gestión de vulnerabilidades se puede desplegar a partir de un modelo de seguridad completo, con una política de seguridad específica asociado a actualizaciones de seguridad que defina lineamientos de operación, roles de usuarios para la ejecución de tareas, documentación detallada, y métricas que permitan la evaluación y clasificación del modelo. Este modelo de seguridad debe ser transversal a todas las capas de servidores en Nube privada y que por lo tanto, permita asegurar las vulnerabilidades a nivel operativo, de servicios, y de aplicaciones y software.

## 4. Modelo de seguridad para la gestión de vulnerabilidades

En la presente tesis de maestría se propone definir un modelo de seguridad para la gestión de vulnerabilidades de servidores en Nubes privadas, conformado por un proceso de aseguramiento apoyado sobre actualizaciones, roles de usuarios y documentación requerida, indicadores de vulnerabilidad basado en factores críticos de seguridad, y clasificación de niveles de seguridad fundamentada en la madurez de la organización.

El modelo de seguridad propuesto contiene las actividades concretas que se deben llevar a cabo para realizar una adecuada gestión de vulnerabilidades tendientes a preservar la confidencialidad, integridad y disponibilidad de la información. Este modelo se centra en una política de seguridad que se conforma siguiendo los requisitos y buenas prácticas presentadas en el Marco de trabajo estructurado para la seguridad de la información en servidores basado en los estándares internacionales ISO/IEC 27000 y O-ISM3 [51]. Esto permite tomar las principales ventajas del marco de trabajo asociadas a establecer las bases para identificar y mitigar vulnerabilidades, definir controles de acceso con privilegios y tareas a realizar por roles de usuarios, especificar la documentación requerida, establecer controles y monitorear el desempeño de los procesos a partir de métricas. Además que tiene la capacidad de adaptarse a distintos tipos de organizaciones y facilita el proceso de certificación de ISO/IEC 27001.

El modelo de seguridad propuesto es transversal a todas las capas de servidores en Nube privada y que por lo tanto, permite asegurar las vulnerabilidades a nivel operativo, de

servicios, y de aplicaciones y software. Este modelo se compone de módulos específicos representados en la Figura 7, que son los siguientes:

- Roles de usuarios.
- Documentación.
- Modelo de proceso de negocio para la gestión de vulnerabilidades.
- Indicadores de vulnerabilidades.
- Modelo de madurez.


**Figura 7.** Módulos del Modelo de Seguridad propuesto.

Además, teniendo en cuenta el nivel de madurez de la organización a partir de los indicadores de vulnerabilidades cuantificados, se proponen un conjunto de recomendaciones de mejora continua para aplicar sobre el modelo, que permitan mejorar su nivel. Su relación se observa en la Figura 8.

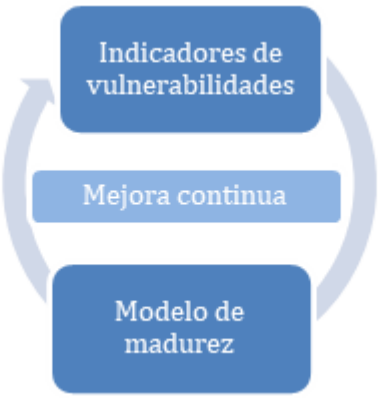



**Figura 8.** Mejora continua para la madurez de la organización.

## Detalle de Política de Seguridad

Si bien es posible aplicar el marco de trabajo a todo tipo de organizaciones que trabajen con sistemas de información computacionales, su implementación es a nivel táctico donde se apunta al diseño, implementación y optimización del sistema de gestión de seguridad de la información, de los objetivos específicos y la gestión de recursos, y no operativo asociado a la ejecución de los procesos y tareas técnicas.

El modelo de seguridad propuesto permite gestionar las vulnerabilidades de servidores en Nubes privadas a nivel táctico y operacional, a partir del marco de trabajo estructurado para la seguridad de la información, mediante la definición de lineamientos de una política de seguridad para gestión de vulnerabilidades de servidores en Nubes privadas que contemple roles de usuarios y documentación a generar, un proceso de gestión de vulnerabilidades que detalle el flujo de actividades a realizar para el aseguramiento de servidores en Nubes privadas, y un esquema de monitoreo de seguridad con indicadores de vulnerabilidad basado en factores críticos de seguridad y clasificación de niveles de seguridad fundamentado en la madurez de la organización.

Como parte de la propuesta de tesis se definen lineamientos generales para el diseño de una política de seguridad basada en la gestión de vulnerabilidades y parches, modelado a partir del marco de trabajo estructurado conformado por el proceso operacional "OSP-05 Actualizaciones de seguridad" que corresponde a la metodología O-ISM3. Además, da

cumplimiento a los controles "12.5 Control del software en explotación" y "12-6 Gestión de la vulnerabilidad técnica" del estándar ISO-27002-2013. En la Tabla 1 se observan los detalles de los lineamientos de política de seguridad propuesto como parte del modelo de seguridad:

| Proceso | Actualizaciones de seguridad |
|---|---|
| Descripción | Descripción del proceso de actualización de servicios tendientes a prevenir incidentes relacionados con vulnerabilidades conocidas, lo que permite mejorar la confiabilidad de los sistemas actualizados. |
| Valor que genera | El análisis de vulnerabilidades permite identificar las amenazas que los activos de información de la organización están expuestos.<br>La aplicación de actualizaciones y parches de seguridad previene incidentes causados por la explotación de una vulnerabilidad conocida en un servicio.<br>El aplicar actualizaciones y parches de forma sistematizada, mantiene en un nivel bajo las vulnerabilidades, generando una reducción en el nivel de amenaza que puede tener un servicio. |
| Documentación | Documento de Política de seguridad.<br>Documentos de Procedimientos de seguridad.<br>Documentos Instructivos de operación sobre herramientas de seguridad.<br>Se detalla en la sección "05.02 Documentación". |
| Entradas | Inventario de Activos. |
| Salidas | Servicios, aplicaciones y servidores actualizados.<br>Reporte de nivel de actualización de los servicios de TI.<br>Reporte de métricas. |
| Modelo | Proceso de aseguramiento de servidores en Nube privada.<br>Se detalla en la sección "05.03 Modelo de proceso". |
| Indicadores de Calidad | ● Frecuencia de escaneo.<br>● Intensidad de escaneo.<br>● Cobertura de autenticación.<br>● Cobertura de activos.<br>● Cobertura de vulnerabilidades. |

| | |
|---|---|
| | Se detalla en la sección "05.04 Indicadores de Vulnerabilidades". |
| Modelo de madurez | • Alta.<br>• Media a alta.<br>• Baja a media.<br>• Baja.<br>• Nula.<br>Se detalla en la sección "05.05 Madurez de VA". |
| Responsabilidad | • Responsable: Jefe de Seguridad Informática.<br>• Supervisor: Jefe de Auditoría Interna<br>Se detalla en la sección "05.01 Roles de usuario". |
| Procesos Relacionados | Proceso de Gestión de Inventario.<br>Proceso de Control de Cambios. |
| Metodologías relacionadas | ISO 27002:2013 Controles 12.5 y 12.6.<br>O-ISM3 Proceso OSP-05. |

**Tabla 1.** Lineamientos de política de seguridad.

## 4.1. Roles de usuario

A partir de la propuesta del marco de trabajo estructurado para la seguridad de la información, basado en ISO/IEC 27000 que destaca la importancia y necesidad de establecer roles de usuarios dentro de la organización, se asignan los siguientes roles de usuarios para el modelo de seguridad propuesto:

- Responsable: Jefe de Seguridad Informática de la organización, encargado de definir los procesos operacionales, las tareas operativas, los documentos requeridos y los objetivos a cumplir.
- Operador: Operarios de sistemas encargados de realizar las tareas operativas sobre las herramientas de seguridad específicas en función del cumplimiento del proceso de seguridad.

- Supervisor: Jefe de Auditoría Interna de la organización, encargado de auditar el cumplimiento de políticas y procedimientos establecidos, como así también, la consecución de las métricas definidas.
- Interesados: Gerencia y Sub-gerencia de la organización quienes revisan el cumplimiento de la política y envían información para métricas de calidad.

Como extensión, se propone para el modelo de seguridad en la gestión de vulnerabilidades de servidores en Nubes privadas, dos subtipos de roles de usuarios que protagonizan el rol de usuario "Operador", representados en la Figura 9. Los mismos son:

- Operador de seguridad: Especialista de seguridad capaz de analizar y procesar vulnerabilidades informáticas.
- Operador de infraestructura: Especialista de infraestructura de servidores, con permisos de administrador sobre cada servidor de Nube privada, que puede realizar tareas como la instalación de actualizaciones, cambios de configuraciones y reinicios de los mismos.

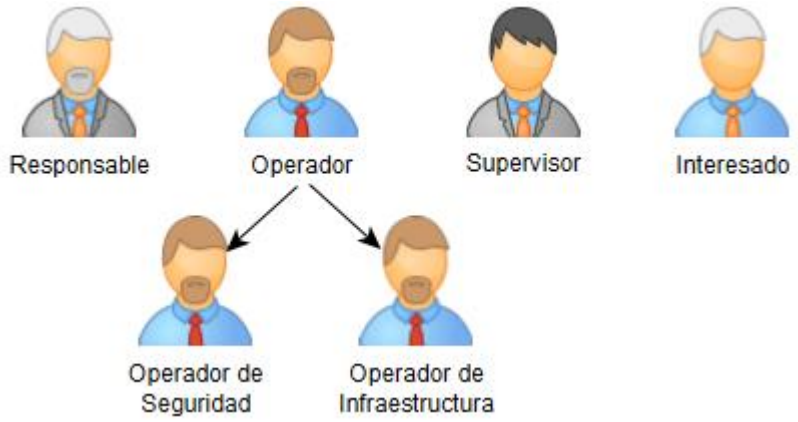



**Figura 9.** Roles de usuarios definidos.

## 4.2. Documentación

La gestión de documentación se alinea con el marco de trabajo estructurado para la seguridad de la información en servidores propuesto en [20], específicamente a su módulo

de gestión de documentación. La misma se basa en los fundamentos del proceso operacional "OSP-05 Actualizaciones de Seguridad" que propone el Estándar O-ISM3 (referirse a Sección 3.1.2) que especifica requerimientos de documentación y repositorios de almacenamiento. Además cumple con los propósitos del dominio "12 Seguridad en la Operativa" que impone el Estándar ISO/IEC 27002 (referirse a Sección 3.1.1) asociado a definir y controlar una estructura de documentos actualizados.

A continuación, se presentan los componentes de documentación:

- Repositorio de documentación:

  **Procesos de Gestión Organizacional**
  - Actualizaciones de Seguridad
    - 01 Documentación
    - 02 Administración
    - 03 Operación
      - 03.01 Reportes
      - 03.02 Registros

- Contenido de cada directorio del repositorio:

  - 01 Bibliografía: Documentación oficial de las herramientas de software utilizadas en la gestión de vulnerabilidades y soluciones de seguridad implementadas para el proceso operacional. Estos documentos son almacenados y actualizados por los usuarios con rol Operador de Seguridad.
  - 02 Administración: Política, procedimientos e instructivos de operación. Dichos documentos son creados y actualizados por los roles Responsable y Operador de Seguridad.
  - 03 Operación: Contiene reportes y registros de las tareas realizadas por los usuarios con rol Operador.

- 03.01 Reportes: Reportes generados por las herramientas y soluciones de software de seguridad utilizadas. Los mismos son almacenados por usuarios con rol Operador.
- 03.02 Registros: Planillas con registros de las operaciones realizadas por usuarios con rol Operador.

- Permisos de acceso en cada directorio:
  - Responsable: Lectura y escritura sobre los directorios "01 Bibliografía", "02 Administración" y "03 Operación".
  - Operador: Lectura sobre los directorios "01 Bibliografía" y "02 Administración", y permiso de lectura y escritura sobre el directorio "03 Operación".
  - Supervisor: Lectura sobre los directorios "01 Bibliografía", "02 Administración" y "03 Operación".

Como parte del modelo de seguridad para la gestión de vulnerabilidades de servidores en Nubes privadas en la presente tesis de maestría, se propone una estructura de documentación específica que contempla clasificación de los documentos, nomenclatura de nombres y tipos de documentos de administración (política, procedimientos e instructivos) y de operación (registros y reportes), con sus plantillas predeterminadas.

Es importante que los documentos de administración y operación, cada uno con sus características, presenten la misma estructura de documentación. Una estructura unificada con información ordenada del mismo modo en los documentos, permite que los usuarios se sientan identificados con la documentación y encuentren de manera más rápida la información. Esto incluye utilizar el mismo formato, color y tipografía para todos los documentos, donde se identifiquen: título, subtítulos y cuerpo de texto.

Como parte de la presente tesis de maestría, se proponen plantillas de documentos que permitan cumplimentar todos los requerimientos delineados. Las plantillas son: Documento de Política, Documento de Procedimiento, Documento de Instructivos, Bitácora de Acciones, Planilla de parches y actualizaciones. Los mismos se representan en la Tabla

2.

| Tipo de Documento | Plantilla |
|---|---|
| **Política** | Documento de política – DP |
| **Procedimiento** | Documento de Procedimiento - DR |
| **Instructivo** | Documento de Instructivo - DI |
| **Operación** | Documento de Operación - DO |
| **Plan de actualizaciones** | Documento de plan de actualizaciones - DA |

**Tabla 2.** Clasificación de documentos.

### Plantilla: Documento de Política

Se propone la realización de un documento de Política de seguridad. En este tipo de documentos se define un conjunto de reglas para el mantenimiento y control de la seguridad de la información como así también el plan de acción para afrontar riesgos de seguridad, siendo el contenido independiente de las herramientas o soluciones de software utilizadas operativamente. Este documento es generado por el usuario con rol Responsable y visualizado por toda la organización. La plantilla del documento se visualiza en Tabla 3.

*Nombre de la política*
Documento de Política

***Nombre de la política***

**Historial de Revisiones**

| Fecha | Versión | Descripción | Autor |
|---|---|---|---|
| DD/MM/ AA | 1.0 | Generación de documento | Nombre y Apellido |
| | | | |

**Definiciones y Glosario**

*DD: Día*

*MM: Mes.*

*AA: Año.*

**Propósito del documento**

Descripción del propósito del documento.

**Política**

| | |
|---|---|
| Descripción | |
| Valor que genera | |
| Documentación | |
| Entradas | |
| Salidas | |
| Modelo | |
| Indicadores de Calidad | |
| Modelo de madurez | |
| Responsabilidad | |
| Procesos Relacionados | |
| Metodologías relacionadas | |

| | | |
|---|---|---|
| Autor: Nombre y Apellido | Clasificación | Página 1 de 1 |

**Tabla 3.** Plantilla: Documento de Política - DP.

Por lo general, la política de seguridad de un proceso operacional no cambia. Solo se pueden llegar a realizar pequeños ajustes con el tiempo, de acuerdo a solicitudes gerenciales o por nuevos procesos que afectan a la política definida.

### Plantilla: Documento de procedimiento

En segunda instancia, se propone la realización de documentos de procedimientos.

Estos documentos se utilizan para definir un conjunto de acciones que tienen que realizarse de la misma forma, para obtener siempre el mismo resultado bajo las mismas circunstancias. Es decir, para estandarizar modos de acción. El contenido desarrollado en los documentos es independiente de las herramientas o soluciones de software utilizadas operativamente. Son documentos redactados por un usuario con rol Operador de Seguridad, revisado por el rol Responsable y utilizado por los Operadores de Infraestructura. Dentro del proceso, los documentos de procedimientos recomendados son:

- Procedimiento para actualizar inventario de activos.
- Procedimiento de alta de servidores para escaneo de vulnerabilidades.
- Procedimiento de baja de servidores para escaneo de vulnerabilidades.
- Procedimiento para obtener y verificar actualizaciones y parches de seguridad.

Se propone la estructura para la realización de documentos de procedimiento en la Tabla 4.

| *Nombre del Documento*<br>Documento de Procedimiento |
|---|

***Nombre del Documento***

**Historial de Revisiones**

| Fecha | Versión | Descripción | Autor |
|---|---|---|---|
| DD/MM/<br>AA | 1.0 | Generación de<br>documento | Nombre y<br>Apellido |
| | | | |

**Índice**



**Definiciones y Glosario**

*DD: Día*

*MM: Mes.*

*AA: Año.*

**Propósito del documento**

Descripción del propósito del documento.

**Procedimiento**

Descripción del procedimiento.

**Flujo de tareas**

Descripción de cada tarea y sus relaciones.

| Autor: Nombre y Apellido | Clasificación | Página 1 de 1 |
|---|---|---|

**Tabla 4.** Plantilla: Documento de Procedimiento - DR.

Los documentos de procedimientos no suelen cambiar. Pueden sufrir ajustes o modificaciones principalmente por cambios en la política de seguridad o por nuevas métricas de performance.

### Plantilla: Documento de instructivo

En tercera instancia, se propone la realización de documentos de instructivos. En estos se detallan tareas operativas a realizar, por cada herramienta o solución de software utilizada en el modelo de seguridad. Las tareas detalladas deben alinearse a la política de seguridad y deben permitir cumplimentar los procedimientos definidos. Estos documentos son redactados por un Operador de Seguridad, revisado por el Responsable y utilizado por Operador de Infraestructura.

Se propone la realización de los siguientes documentos de operación:

- Instructivo para actualizar la base de firmas en herramienta.
- Instructivo para instalar parches en servidores de Nube privada.
- Instructivo para instalar actualización en servidores de Nube privada.

Se propone la estructura para la realización de documentos de instructivos de operación

en la Tabla 5.

| *Nombre del Documento*<br>Instructivo de Operación |
|---|

## *Nombre del Documento*

### Historial de Revisiones

| Fecha | Versión | Descripción | Autor |
|---|---|---|---|
| DD/MM/AA | 1.0 | Generación de documento | Nombre y Apellido |
| | | | |

### Índice



### Definiciones y Glosario

*DD: Día*

*MM: Mes.*

*AA: Año.*

### Propósito del documento

Descripción del propósito del documento.

### Herramientas de seguridad

Descripción de las herramientas y software de seguridad.

### Flujo de tareas

Descripción de cada tarea y sus relaciones.

| Autor: Nombre y Apellido | Clasificación | Página 1 de 1 |
|---|---|---|

**Tabla 5.** Plantilla: Documento de Instructivo de Operación - DI.

### Plantilla: Documento de operación

En cuarta instancia, se propone la realización de documentos de operación llamados Bitácoras. En estos se detallan tareas operativas a ser ejecutadas, por cada herramienta o solución de software utilizada en el proceso. Se detalla la fecha, hora, usuario y tarea realizada. Este documento es de gran utilidad para tener un seguimiento de las tareas que realiza cada usuario en el proceso. Estos documentos son completados por usuarios con rol Operador, tanto Operador de Seguridad como Operador de Infraestructura, ya que son quienes realizan las tareas operativas en el modelo de seguridad.

Se propone una estructura de hoja de cálculo para la realización de documentos de operación. En la Tabla 6 se observa la plantilla para la carátula del documento y en la Tabla 7 se observa la plantilla de las pestañas del documento donde los operadores deben completar las acciones.

| | | | | |
|---|---|---|---|---|
| *Nombre del Documento*<br>Documento de Operación | | | | |
| **Nombre del Documento** | | | | |
| **Historial de Revisiones** | | | | |
| **Fecha** | **Versión** | **Descripción** | **Autor** | |
| DD/MM/AA | 1.0 | Generación de documento | Nombre y Apellido | |
| | | | | |
| **Índice** | | | | |
| Carátula | 1 | | | |
| Pestaña 1 | 2 | | | |
| Pestaña 2 | 3 | | | |
| | | | | |
| **Definiciones y Glosario** | | | | |
| DD | Día | | | |
| MM | Mes | | | |
| AA | Año | | | |
| | | | | |
| **Propósito del documento** | | | | |
| Descripción del propósito del documento. | | | | |
| | | | | |

**Tabla 6.** Plantilla: Carátula de documento de Operación - DO.

| ID | Fecha | Descripción | Autor |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | DD/MM/AA | Detalle operación 1. | Nombre y Apellido |
| 2 | DD/MM/AA | Detalle operación 2. | Nombre y Apellido |
| 3 | DD/MM/AA | Detalle operación 3. | Nombre y Apellido |

**Tabla 7.** Plantilla: Cuerpo de documento de Operación - DO.

### Plantilla: Documento de plan de actualizaciones

En quinta y última instancia, se propone la realización de documento planilla de parches y actualizaciones, utilizado para realizar e indicar el plan de actualizaciones. Este documento es generado por un Operador de Seguridad y utilizado por un Operador de Infraestructura para liberar e instalar los parches y actualizaciones indicadas en el mismo.

Se propone una estructura de hoja de cálculo para la realización de este documento. En la Tabla 8 se observa la plantilla para la carátula del documento y en la Tabla 9 se observa la plantilla de las pestañas del documento donde los operadores deben completar las acciones. Habrá una nueva pestaña por cada mes. En este documento es importante identificar el CVE de la vulnerabilidad, el KB de mitigación y el sistema operativo afectado.

| | | | | |
|---|---|---|---|---|
| *Nombre del Documento*<br>Plan de actualizaciones | | | | |
| **Nombre del Documento** | | | | |
| **Historial de Revisiones** | | | | |
| **Fecha** | **Versión** | **Descripción** | **Autor** | |
| DD/MM/AA | 1.0 | Generación de documento | Nombre y Apellido | |
| | | | | |
| **Índice** | | | | |
| Carátula | 1 | | | |
| Pestaña 1 | 2 | | | |
| Pestaña 2 | 3 | | | |
| | | | | |
| **Definiciones y Glosario** | | | | |
| DD | Día | | | |
| MM | Mes | | | |
| AA | Año | | | |
| | | | | |
| **Propósito del documento** | | | | |

| Descripción del propósito del documento. | | | | |
|---|---|---|---|---|
| | | | | |

**Tabla 8.** Plantilla: Carátula de documento de Plan de actualizaciones - DA.

| Orden | CVE | KB | Sistema Operativo | Vulnerabilidad resuelta |
|---|---|---|---|---|
| 1 | | KB999999 | | |
| 2 | | KB999999 | | |
| 3 | | KB999999 | | |

**Tabla 9.** Plantilla: Cuerpo de documento de Plan de actualizaciones - DA.

## 4.3. Proceso de gestión de vulnerabilidades

La detección de vulnerabilidades como así también la distribución e instalación de actualizaciones y parches de los servidores en Nubes privadas, ya sean de seguridad o de funcionalidad, debe estar guiada por un proceso de gestión de vulnerabilidades que identifique adecuadamente el ciclo de vida e indique su periodicidad [53].

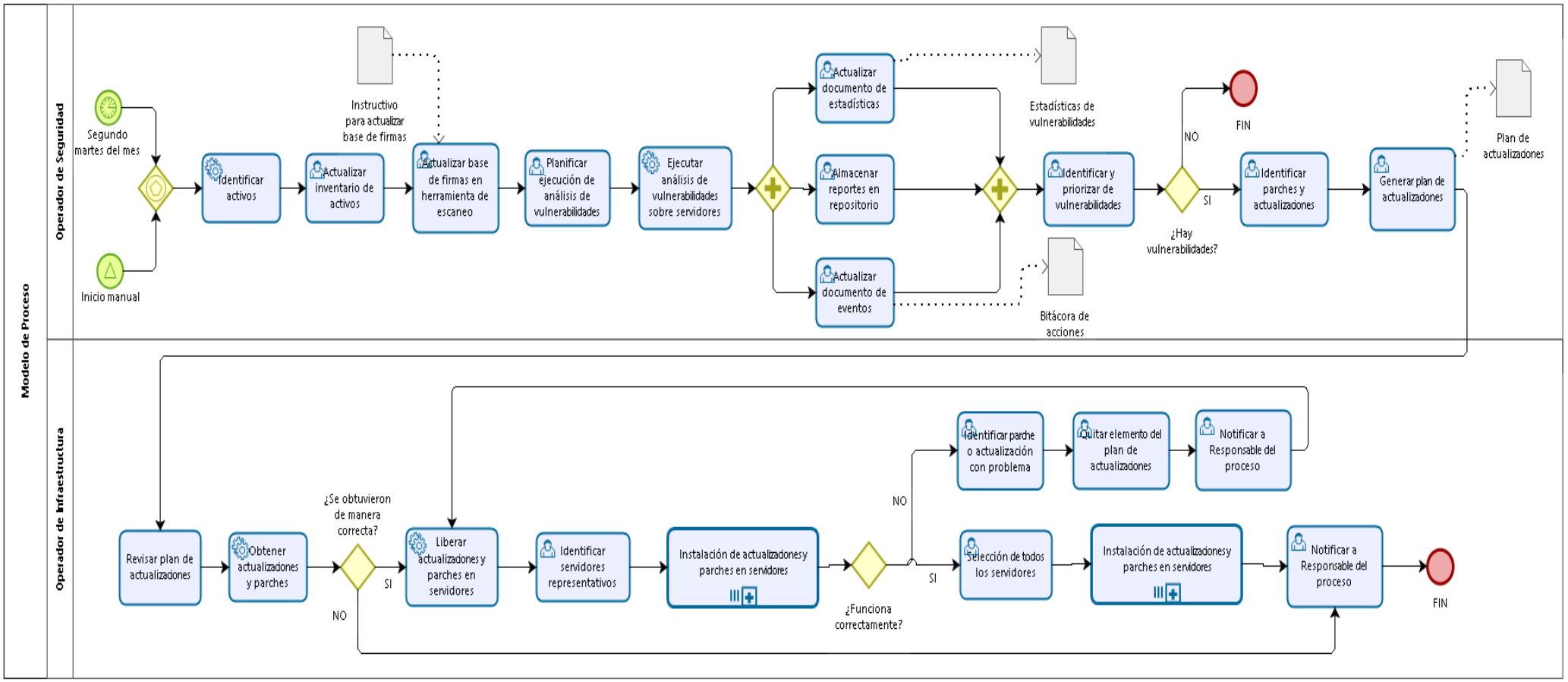
Una estrategia efectiva de gestión de vulnerabilidades es fundamental para distribuir actualizaciones de software y, lo que es más importante, para detectar y reparar las vulnerabilidades de seguridad. Muchos ataques exitosos se cometen contra las vulnerabilidades previamente conocidas para las que el proveedor de software ya disponía de una revisión o estándar de configuración segura. Sin embargo, estos parches únicamente son efectivos si se han implementado [54].

Como parte del modelo de seguridad, se propone un proceso de gestión de vulnerabilidades para servidores en Nubes privadas, basado en los lineamientos generales de la política de seguridad definida en la sección 4, en lo que respecta a roles de usuarios, documentación requerida y objetivos de seguridad. Este proceso está apoyado en los fundamentos del proceso operacional "OSP-05 Actualizaciones de Seguridad" que propone el Estándar O-ISM3 (Referirse a Sección 3.1.2) y cumple con los objetivos de control especificados en el punto "12.6 Gestión de la vulnerabilidad técnica", requeridos por el Estándar ISO/IEC 27002 (Referirse a Sección 3.1.1). Además, se alinea con el marco de trabajo estructurado para la seguridad de la información en servidores propuesto en [20],

específicamente a su módulo de gestión de vulnerabilidades, el cual define un ciclo de vida de seis fases: Identificación, Disponibilidad, Aplicabilidad, Adquisición, Validación y Despliegue (Referirse a Sección 3.2.3).

### Modelo de proceso de negocio para la gestión de vulnerabilidades

El proceso de gestión de vulnerabilidades para servidores en Nubes privadas se representa gráficamente en la Figura 10 mediante la técnica de notación gráfica Business Process Model and Notation (BPMN). La elección de esta técnica se basa en que con BPMN es posible especificar un proceso en un diagrama en el que es fácil de leer tanto para los usuarios técnicos como para los usuarios de negocios. Es intuitivo y permite la representación de los detalles complejos del proceso, ya que provee perspectivas de flujo de control, de datos (documentos) y permite el modelado de recursos y excepciones, dando soporte a todos los conceptos del modelo de seguridad propuesto. Además, los modelos de proceso de negocio pueden ser interpretados y ejecutados por sistemas de gestión de procesos de negocio permitiendo la automatización de las actividades. Sirve como un lenguaje estándar, lo que resuelve el problema definido a la falta de comunicación entre el modelado de procesos y su ejecución. Es destacable que BPMN es un lenguaje que puede ser extendido, lo que permite en trabajos futuros anexar al mismo los conceptos del modelo de seguridad propuestos en esta tesis. Por último, se destaca que en la actualidad existe una gran tendencia a que las organizaciones utilicen este tipo de sistemas en distintas áreas, lo que permitiría agilizar su implementación. Para más detalles sobre la elección del lenguaje de modelado como de la semántica de BPMN, referirse a "*Anexo II – Lenguaje de Modelado*"


Modelo de Proceso
Operador de Seguridad
Operador de Infraestructura
Segundo martes del mes
Inicio manual
Identificar activos
Actualizar inventario de activos
Instructivo para actualizar base de firmas
Actualizar base de firmas en herramienta de escaneo
Planificar ejecución de análisis de vulnerabilidades
Ejecutar análisis de vulnerabilidades sobre servidores
Actualizar documento de estadísticas
Almacenar reportes en repositorio
Actualizar documento de eventos
Estadísticas de vulnerabilidades
Bitácora de acciones
Identificar y priorizar de vulnerabilidades
¿Hay vulnerabilidades?
NO
FIN
SI
Identificar parches y actualizaciones
Generar plan de actualizaciones
Plan de actualizaciones
Revisar plan de actualizaciones
Obtener actualizaciones y parches
¿Se obtuvieron de manera correcta?
NO
SI
Liberar actualizaciones y parches en servidores
Identificar servidores representativos
Instalación de actualizaciones y parches en servidores
¿Funciona correctamente?
NO
SI
Identificar parche o actualización con problema
Quitar elemento del plan de actualizaciones
Notificar a Responsable del proceso
Selección de todos los servidores
Instalación de actualizaciones y parches en servidores
Notificar a Responsable del proceso
FIN

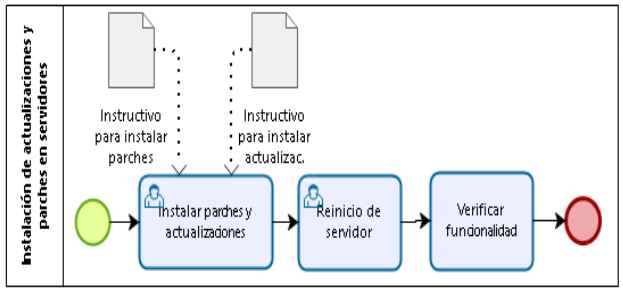

Instalación de actualizaciones y parches en servidores
Instructivo para instalar parches
Instructivo para instalar actualizac.
Instalar parches y actualizaciones
Reinicio de servidor
Verificar funcionalidad

**Figura 10.** Modelado con BPMN de proceso con marco de trabajo.

El proceso puede iniciar en cualquier momento por iniciativa del Operador de Seguridad o de manera automática cada segundo martes de mes. El inicio automático se corresponde con la publicación de los boletines de seguridad de Microsoft. Si bien el proceso contempla actualizaciones y parches de todos los fabricantes de software, se considera este punto temporal de inicio debido a que Microsoft es el único que tiene definida una fecha segura de liberación. Además, estadísticas a nivel global, muestran que la mayor parte de las organizaciones utilizan tanto los sistemas operativos como aplicaciones de este fabricante en entornos de Nubes privadas [3].

De esta manera el proceso da inicio a la primera fase del módulo de Gestión de Vulnerabilidades (Identificación), en la cual un Operador de Seguridad debe identificar todos los activos de la organización, incluyendo los servidores en Nube privada, como así también las aplicaciones y software instalados. Con la información recopilada, debe relevar el inventario de activos. La relevación del inventario puede ser realizada de manera automática con una herramienta de software específica para tal fin o de manera manual por un Operador de Seguridad, quién es el responsable de la tarea.

Luego, el proceso continúa con la segunda fase del módulo de Gestión de Vulnerabilidades (Disponibilidad), que se centra en detectar vulnerabilidades sobre todos los servidores relevados en el inventario de activos. Para esto, el Operador de Seguridad debe actualizar la base de firmas de la herramienta de análisis de vulnerabilidades, lo que permite que en su ejecución tenga disponible los patrones de las nuevas amenazas publicadas. Una vez actualizada, debe planificar en fecha y hora la ejecución del análisis para cada uno de los servidores en Nube privada, lo que permitirá detectar las vulnerabilidades expuestas en cada uno. Es importante tener en cuenta que la herramienta de escaneo ocasiona una alta utilización de recursos de hardware en cada servidor, por lo que se recomienda planificar su ejecución en un horario donde tenga una baja carga de utilización, acordado con el operador de infraestructura.

Al finalizar el análisis de vulnerabilidades, el operador de seguridad puede realizar tres tareas en paralelo. Estas tareas se deben ejecutar a partir de los resultados obtenidos del

análisis de vulnerabilidades, donde se detallan todas las vulnerabilidades detectadas como así también los parches y actualizaciones recomendados por las herramientas de escaneos, para instalar o aplicar en los servidores de la Nube privada. Las actividades son:

- Almacenar los reportes con resultados obtenidos de los análisis de vulnerabilidades en cada servidor, en un repositorio interno (Repositorio "03.01 Reportes").
- Actualizar documentos donde se registre una bitácora de las acciones que son realizadas (Documento de operación llamado Bitácora de acciones).
- Actualizar un documento de estadística de análisis de vulnerabilidades mensuales realizados (Documento de operación llamado Estadísticas de vulnerabilidades).

A continuación, el proceso continúa con la tercera fase del módulo de Gestión de Vulnerabilidades (Aplicabilidad), en la cual los resultados de los análisis deben ser identificados y priorizados por el Operador de Seguridad para detectar las vulnerabilidades por cada servidor en la Nube privada. Aquí este Operador debe priorizar las mismas dependiendo de su nivel de criticidad e importancia, de acuerdo a la categorización de las características CVE (referirse a sección 2.2.1). Si ocurre que no se detectan vulnerabilidades, finaliza el proceso operacional con éxito. En caso contrario, a partir de las vulnerabilidades detectadas, el Operador de Seguridad debe identificar las actualizaciones y los parches de seguridad publicados, que permitan mitigar dichas vulnerabilidades. Con esta información, el operador de seguridad debe generar un plan de actualizaciones que contenga una lista con todos los parches requeridos por cada servidor en la Nube privada como así también las actualizaciones de software requeridas, teniendo en cuenta todas las vulnerabilidades analizadas. Este plan de actualizaciones se deriva posteriormente a un Operador de Infraestructura quién continuará el proceso.

En la cuarta fase (Adquisición), el Operador de Infraestructura recibe y revisa el plan de actualizaciones generado por el Operador de Seguridad. Luego utiliza una herramienta de administración de actualizaciones y parches del cual obtiene las actualizaciones y parches, del cual lo puede hacer de manera manual o semi-automatizada, dependiendo de las

funcionalidades de la herramienta utilizada. En esta instancia, es importante que verifique que sea de una fuente oficial y fidedigna, para no generar problemas secundarios en su uso. De este modo, una vez que el operador descarga todas las actualizaciones y parches requeridos de manera correcta, realiza la liberación de los mismos para que sean distribuidos a todos los servidores afectados en la Nube privada.

El proceso continúa con la quinta fase del módulo de Gestión de Vulnerabilidades (Validación), en la cual a partir del momento en que el operador de infraestructura cuenta con las actualizaciones y parches que resuelven o mitigan las vulnerabilidades detectadas como resultado de los análisis efectuados, debe identificar servidores representativos dentro para luego realizar la instalación de actualizaciones y parches en los mismos. Esto responde a una buena práctica de verificar el funcionamiento y/o mejoras de cada actualización o parche en cuestión, para que no impacte en toda la infraestructura de servidores en Nube privada en caso de que tenga algún problema, ya sea de incompatibilidad, performance, entre otros. Este grupo reducido de servidores en Nube privada debe ser seleccionado del inventario de activos, considerando aquellos de menor importancia, criticidad o impacto que pueda llegar a generar. Es importante que este grupo sea representativo con respecto a toda la infraestructura en Nube, de modo que se verifique el funcionamiento de todo el software y servicios que se brindan. Teniendo identificados los servidores representativos y liberados los parches y actualizaciones para su uso, el Operador de Infraestructura debe realizar las siguientes tareas por cada servidor: instalar parches y actualizaciones siguiendo los lineamientos de los documentos Instructivo para instalar parches e Instructivo para instalar actualizaciones, reiniciar el servidor en caso de ser necesario, y finalmente verificar las funcionalidades afectadas con el cambio.

En la sexta y última fase (Despliegue), una vez que las actualizaciones y parches fueron verificados en servidores de baja criticidad, y están distribuidas en todos los activos comprometidos, el Operador de Infraestructura procede a realizar la instalación de actualizaciones y parches en todos y cada uno de estos servidores de manera similar al realizado con los servidores representativos: instalación siguiendo los lineamientos de los documentos Instructivo para instalar parches e Instructivo para instalar actualizaciones, reinicio y verificación de funcionalidades afectadas.

Una vez finalizadas todas las tareas, el operador de seguridad debe notificar mediante correo electrónico lo realizado al Responsable del proceso, con el cual se da por terminado el proceso.

Dentro del proceso pueden ocurrir situaciones no deseadas o excepciones:

- Falla la instalación de actualización o parche: Puede ocurrir cierta incompatibilidad en la instalación de una actualización o parche con el sistema operativo del servidor en Nube privada, lo que genera que el mismo no pueda ser instalado. En este caso, el operador de infraestructura debe notificar al responsable del proceso el problema y se debe asumir la vulnerabilidad como no controlable. El responsable puede evaluar otras opciones o esquemas de seguridad que puedan mitigar dicha vulnerabilidad.

- No es posible obtener actualización o parche: Es posible que una vulnerabilidad esté asociada a una actualización o parche específico como mitigación a la misma, y que éste no sea posible obtenerlo o ya esté deprecado. Estos casos son comunes con software o sistemas operativos obsoletos, que están fuera del soporte del fabricante. El operador de infraestructura debe notificar al responsable del proceso el problema y se debe asumir la vulnerabilidad como no controlable.

- Falla funcionamiento de actualización o parche instalado: Si una actualización o parche instalado genera problemas sobre el funcionamiento del servidor o en los servicios que brinda, se debe quitar de la lista de distribución. Para esto, el operador de infraestructura debe notificar mediante correo al operador de seguridad indicando el problema y este último debe quitarlo de la lista de distribución de actualizaciones y parches. Además, debe notificar al referente del proceso y documentar el problema para que no vuelva a ocurrir.

## 4.4. Indicadores de Vulnerabilidades

Durante la primera fase de Identificación, los activos se individualizan y mapean para lograr visibilidad en cualquier entorno informático. Además, supone comprender el estado de todos los activos, incluso las vulnerabilidades, configuraciones erróneas y otros indicadores de estado. Es una fase de suma importancia debido a que determina decisivamente el alcance y el ritmo de las fases posteriores, como la determinación de prioridades y la reparación.

La evaluación de vulnerabilidades se lleva a cabo mediante la implementación de un escáner para evaluar los activos de forma remota a través de la red, al interrogar los parches instalados, los puertos abiertos y los servicios disponibles para determinar si son vulnerables.

Se detallan a continuación las consideraciones principales a tener en cuenta durante la evaluación de vulnerabilidades para lograr un proceso eficaz:

- Escanear lo suficiente para cumplir con los requisitos reglamentarios.
- Escanear con la mayor frecuencia posible para minimizar el período de tiempo en el que una vulnerabilidad crítica puede residir en su entorno sin su conocimiento y para obtener información actualizada sobre evaluación comparativa y la inteligencia de asignación de puntaje a los riesgos.
- Obtener tanta visibilidad de las vulnerabilidades críticas de los activos como sea posible y comenzar con evaluaciones remotas sin credenciales y progresando cada vez más hacia el uso de la autenticación.
- Evaluar la mayor cantidad de infraestructura posible y extenderse a través de todos los activos, las tecnologías y las aplicaciones implementados para reducir la superficie de ataque disponible a la que un adversario pueda apuntar.
- Aprovechar las plantillas de escaneo personalizadas para adaptar las evaluaciones a grupos de activos, unidades de negocio y casos de uso específicos para reducir los gastos generales de escaneo y los falsos positivos, así como para limitar la complejidad innecesaria.

Como parte de la presente tesis de maestría, se detectaron cinco factores críticos que están relacionados con la forma en que se ejecuta el análisis de vulnerabilidades: frecuencia

de escaneo, intensidad de escaneo, cobertura de autenticación, cobertura de activos y cobertura de vulnerabilidades. Estos se reconocen como indicadores de rendimiento de la evaluación de vulnerabilidades y se corresponden con la madurez del procedimiento. El detalle de los cinco indicadores se observa en la Tabla 10.

| Indicadores de rendimiento de evaluación de vulnerabilidades | Detalle |
|---|---|
| Frecuencia de escaneo | Indicador que mide la regularidad con la que se realizan evaluaciones en función del tiempo promedio entre los días en que se ejecuta un escaneo (día del escaneo). Una mayor frecuencia supone menos días entre evaluaciones y, en consecuencia, significa que las vulnerabilidades críticas se pueden identificar más rápidamente.<br>La frecuencia de escaneo se clasifica en:<br>● Bajo: Dos o menos escaneos por mes.<br>● Moderado: Escaneo semanal.<br>● Alto: Más de un escaneo por semana. |
| Intensidad de escaneo | Indicador de escaneo que mide cuántos escaneos diferentes se inician en un día de escaneo determinado. Una mayor intensidad de escaneo indica que se ejecuten múltiples escaneos, ya sea que se utilicen varios escáneres o porque están usando plantillas de escaneo diferenciadas y personalizadas para abarcar diferentes grupos de activos, familias tecnológicas o casos de uso.<br>La intensidad de escaneo se clasifica en:<br>● Bajo: Un único escaneo determinado.<br>● Moderado: Entre dos y cuatro escaneos diferentes.<br>● Alto: Cinco o más escaneos determinados. |
| Cobertura de autenticación | El indicador de cobertura de autenticación es una medición de la profundidad de la evaluación, y se logra brindando credenciales de usuario con privilegios del servidor a la herramienta de análisis. Las evaluaciones no autenticadas solo proporcionan una visión muy |

| | |
|---|---|
| | limitada y parcial, que el escaneo con credenciales.<br>La cobertura de autenticación se clasifica en:<br>● Bajo: Menos del 30 % de los escaneos incluyen credenciales de autenticación.<br>● Moderado: Entre el 30 % y el 70 % de los escaneos incluye credenciales de autenticación.<br>● Alto: Más del 70 % de los escaneos incluyen credenciales de autenticación. |
| Cobertura de activos | Indicador que mide la proporción de los activos escaneados en un período de **30** días, con respecto al total que contiene la organización.<br>● Bajo: Menos del 30 % de todos los activos se evalúan en un período de 90 días.<br>● Moderado: Entre el 30 % y el 70 % de los activos se evalúan en un período de 90 días.<br>● Alto: Más del 70 % de los activos se evalúan en un período de 90 días. |
| Cobertura de vulnerabilidades | Indicador que mide la proporción de vulnerabilidades totales utilizadas en un período de 30 días. Esto indica la exhaustividad general de las evaluaciones en la cobertura de diversas tecnologías y familias de vulnerabilidades.<br>● Bajo: Menos del 25 % de todos los complementos de vulnerabilidades disponibles.<br>● Moderado: Entre el 25 % y el 75 % de todos los complementos de vulnerabilidades disponibles.<br>● Alto: Más del 75% de todos los complementos de vulnerabilidades disponibles. |

**Tabla 10.** Indicadores de rendimiento de la evaluación de vulnerabilidades.

## 4.5. Modelo de Madurez

A partir de los indicadores de vulnerabilidades, se proponen como parte de la presente tesis de maestría, cinco niveles de madurez. Los niveles de madurez proporcionan la base para una mejora continua del proceso operacional del modelo de seguridad en la organización y se miden por el logro en el cumplimiento de todos los indicadores de rendimiento. Estos niveles se caracterizan de la siguiente manera:

- **Nivel 0: Madurez nula**
  Ejecuta mínimamente evaluaciones de vulnerabilidades que no cumplen mandatos normativos.
  - Escaneo de manera ad hoc, no llega a una corrida por mes.
  - Realiza un solo escaneo a la vez.
  - Cobertura de activos menor al 20% del total.
  - No utiliza autenticación en los escaneos.
  - No desarrolla plantillas sino que usa las predeterminadas.

- **Nivel 1: Madurez baja**
  Ejecuta evaluaciones de vulnerabilidades mínimas como lo exigen los mandatos de cumplimiento normativo.
  - Escaneo mensual.
  - Cobertura de activos mayor a 20% y menor al 40% del total.
  - Autenticación hasta el 25% de los activos analizados.
  - Aprovecha una sola plantilla de escaneo.

- **Nivel 2: Madurez baja a media**
  Realiza evaluaciones de vulnerabilidades de amplio alcance de manera frecuente, pero se enfoca principalmente en un subconjunto de vulnerabilidades.
  - Escaneo semanal (al menos más de una vez por mes).
  - Cobertura de activos menor al 60% del total.
  - Autenticación entre el 25% y el 50% de los activos analizados.

- **Nivel 3: Madurez media a alta**
  Lleva a cabo evaluaciones de vulnerabilidades con un alto nivel de madurez, pero solo evalúa activos específicos.
  - Escaneo semanal.

- Escaneos distribuidos o específicos de un caso de uso.
- Cobertura de activos menor al 80% del total.
- Autenticación entre el 50% y el 75% de los activos analizados.
- Aprovecha varias plantillas de escaneo optimizadas y dirigidas.

- **Nivel 4: Madurez alta**
  Lleva a cabo evaluaciones de vulnerabilidades integrales y adapta los escaneos según el caso de uso, pero solo auténtica selectivamente.
  - Escanea múltiples veces por semana.
  - Ejecuta muchos escaneos segmentados o diferenciados.
  - Cobertura de activos mayor al 80% del total.
  - Autenticación en todos los escaneos.
  - Aprovecha distintas plantillas de escaneo para diferentes casos de uso.

Los niveles de madurez se relacionan directamente con el grado de cumplimiento de los indicadores de rendimiento de la evaluación de vulnerabilidades. Esta relación se observa en la Tabla 11.

| Nivel | Frecuencia de escaneo | Intensidad del escaneo | Cobertura de autenticación | Cobertura de activos | Cobertura de vulnerabilidades |
|---|---|---|---|---|---|
| **0** | Nulo | Nulo | Nulo | Nulo | Nulo |
| **1** | Bajo | Bajo | Nulo | Bajo | Bajo |
| **2** | Moderado | Moderado | Bajo | Moderado | Bajo |
| **3** | Moderado | Moderado | Moderado | Moderado | Moderado |
| **4** | Alto | Alto | Alto | Alto | Alto |

**Tabla 11.** Relación entre niveles de madurez e indicadores de rendimiento.

A Cabe destacar que deben cumplirse los cinco indicadores para que corresponda al nivel de madurez adecuado. Si no se cumple con alguno de los indicadores, el modelo implementado disminuye su nivel de madurez al nivel en que se encuentra el indicador específico. Por ejemplo, si en el cálculo de indicadores de un modelo implementado, todos tienen como resultado factor Alto excepto uno de ellos que es factor Moderado, el modelo de madurez resultará en Nivel 3, y no nivel 4.

## 4.6. Mejora continua

A partir del modelo de madurez al que aplica una organización en particular posterior a analizar el cumplimiento de los indicadores de vulnerabilidades, pensando en la mejora continua, existen un conjunto de recomendaciones a seguir para crecer a un mejor nivel de madurez. Las recomendaciones generales se centran en: reducción de tiempo entre escaneos, utilización de diferentes herramientas de análisis de vulnerabilidades, autenticación en el escaneo para tener un análisis exhaustivo, ampliación en la cantidad de activos y utilización de plantillas personalizadas de escaneo para lograr mayor especificidad.

El ideal de activos a analizar es el total de la infraestructura, y en caso de que esto no pueda llevarse a cabo, es importante seleccionarlos cuidadosamente a partir de la priorización de los mismos. El criterio de selección está asociado con el nivel de importancia y criticidad que los activos tienen en la organización. Los indicadores analizados por los administradores de activos al seleccionar los de mayor importancia para incluirlos al ciclo de gestión de vulnerabilidades son: nivel de exposición a la red externa, importancia del servicio brindado, criticidad de los datos que contiene y nivel de obsolescencia del servidor como de su software.

Además de las consideraciones generales brindadas, se proponen las siguientes recomendaciones de alto nivel que se deben aplicar para mejorar la madurez de análisis de vulnerabilidades de la organización, lo que permitirá pasar al siguiente nivel:

- **De Nivel 0 a Nivel 1:**

Establecer un programa de evaluaciones periódicas al menos con una periodicidad mensual y dejar de trabajar de manera ad hoc.

Definir un conjunto de activos a analizar, superando al 20% del total. Inicialmente se puede priorizar teniendo en cuenta el nivel de criticidad en el negocio y el grado de exposición.

- **De Nivel 1 a Nivel 2:**

Reducir la cantidad de días entre las evaluaciones periódicas, pasando de escaneos mensuales a escaneos semanales.

Ampliar la cobertura de activos a grupos de activos, superando el 40% de activos respecto del total que dispone la organización.

Aprovechar credenciales para el escaneo autenticado en al menos el 25% de los servidores en Nube privada, a fin de obtener una visión más profunda y confiable de las vulnerabilidades de un activo.

Comenzar a aprovechar el escaneo distribuido para equilibrar las evaluaciones en varios escáneres y para reducir la duración del escaneo.

- **De Nivel 2 a Nivel 3:**

Superar el 60% de activos a los que se le da cobertura con el proceso.

Ampliar el uso de credenciales, superando el 50% de escaneos autenticados, a fin de lograr una visión más profunda y confiable de las vulnerabilidades de un activo.

Aprovechar las plantillas de escaneo personalizadas que se centran en familias tecnológicas específicas y para casos de uso específicos, como las vulnerabilidades aprovechables.

- **De Nivel 3 a Nivel 4:**

Ampliar la cobertura de activos a la organización en general, superando el 80% de los existentes del total.

Aumentar la frecuencia de escaneo, logrando que sea más de una vez por semana,

para minimizar el tiempo que lleva tomar conocimiento de vulnerabilidades críticas y responder a ellas.

Lograr que todos los escaneos se realicen con autenticación de usuario.

Ampliar el uso de plantillas de escaneo personalizadas que se centran en familias tecnológicas específicas y para casos de uso específicos, por ejemplo, para vulnerabilidades aprovechables.

- **Mejora continua Nivel 4:**

Ampliar el escaneo autenticado (basado en credenciales) más allá de activos y tecnologías específicas, llegando al 100% de servidores en Nube privada de la organización.

Incluir todas las tecnologías existentes como aquellas no tradicionales en el alcance de su programa de gestión de vulnerabilidades, como activos web, en la nube, virtual y móvil.

## 5. Caso de implementación

En el presente capítulo se muestra una implementación en una organización privada del modelo de seguridad para la gestión de vulnerabilidades de servidores en Nubes privadas propuesto en la presente tesis. Por cuestiones de privacidad no se brinda el nombre de la organización, a la cual en esta tesis se referencia como *Enterprise S.A.* Inicialmente se detalla el marco temporal de la implementación, una descripción de lo realizado por organizaciones sin un modelo de seguridad y sus consecuencias, el paso a paso operacional del modelo de seguridad junto con los indicadores de vulnerabilidades y madurez de la organización, y conclusiones de la implementación.

## 5.1. Contexto

El 15 de marzo de 2017, como cada segundo martes del mes, Microsoft publicó boletines de seguridad donde presentó vulnerabilidades detectadas sobre sus productos y liberó actualizaciones que resuelven estos problemas detectados.

La publicación de marzo constó de 18 boletines de seguridad, clasificados como 9 críticos y 9 importantes, referentes a múltiples vulnerabilidades en Microsoft Internet Explorer, Microsoft Windows, Microsoft Office, Windows DVD Maker, Windows DirectShow, Adobe Flash Player y Microsoft Edge.

Como solución a las vulnerabilidades presentadas, Microsoft recomendó instalar la actualización correspondiente. En el resumen de los boletines de seguridad de Microsoft, se informa de los distintos métodos de actualización dentro de cada boletín en el apartado "Información sobre la actualización" [55]. El listado de los boletines publicados en marzo de 2017 es el siguiente:

- MS17-006: Crítica.
- MS17-007: Crítica.
- MS17-008: Crítica.
- MS17-009: Crítica.
- MS17-010: Crítica.
- MS17-011: Crítica.
- MS17-012: Crítica.
- MS17-013: Crítica.
- MS17-014: Importante.
- MS17-015: Importante.
- MS17-016: Importante.
- MS17-017: Importante.
- MS17-018: Importante.
- MS17-019: Importante.
- MS17-020: Importante.
- MS17-021: Importante.

- MS17-022: Importante.
- MS17-023: Crítica.

Dentro de los boletines listados, se destacó el detallado a continuación, debido a que a partir de sus vulnerabilidades, se desarrolló la explotación de diversos ataques mundiales [56]:

- MS17-010: Actualización de seguridad que resuelve varias vulnerabilidades en Microsoft Windows. La más grave de ellas puede permitir la ejecución remota de código si un atacante envía un mensaje manipulado a Microsoft Server Message Block 1 (SMBv1). Se recomienda la instalación del parche KB4013389.

## 5.2. Infección de Ransomware

A partir de la vulnerabilidad en la implementación del protocolo Server Message Block (SMB) publicada por Microsoft en el boletín MS17-010 y aprovechando un exploit desarrollado por la NSA en los Estados Unidos que se filtró, un grupo de hackers conocido como Shadow Brokers ejecutó el 12 de Mayo de 2017 un ataque mundial de Ransomware con el nombre WannaCry (Referirse a sección 2.2).

Este ataque infectó a más de 230.000 ordenadores en más de 150 países y generó costos totales de alrededor de 4 mil millones de dólares. El punto importante de este ataque, es que si estos servidores que resultaron infectados, hubiesen aplicado el parche KB4013389 que se publicó en el boletín MS17-010 como modo de mitigar la vulnerabilidad, el exploit no hubiese tenido éxito.

A pesar de que el de WannaCry hasta el momento había sido uno de los ataques informáticos más importantes en la historia de los sistemas de información, el 27 de Junio de 2017 se volvió a ejecutar a nivel mundial un nuevo ataque de Ransomware con la variante Petya apoyado en la misma vulnerabilidad de SMBv1 que infectó nuevamente a grandes cantidades de servidores que aún no tenían el parche instalado.

## 5.3. Sin modelo de seguridad

Las organizaciones que no presentan un modelo de seguridad definido con un proceso de seguridad para la gestión de vulnerabilidades, afrontan una enorme cantidad de amenazas de seguridad que pueden afectar su infraestructura informática.

A continuación se detalla un caso genérico, del modo en el que ocurrió en marzo de 2017 cuando se publicó la vulnerabilidad que dio inicio al Ransomware WannaCry, en una organización que no presenta un modelo de seguridad definido.

A partir de la publicación de los boletines de seguridad, las herramientas de actualizaciones automáticas de Microsoft comenzaron a descargar e instalar los parches recomendados por este fabricante para cada sistema operativo. Los boletines con parches recomendados se observan en la Figura 11:

**Suggested Remediations**

| Action to take | Vulns | Hosts |
|---|---|---|
| Install MS17-017 | 2 | 1 |
| Install MS17-011 | 2 | 1 |
| Install MS17-006 | 2 | 1 |

**Figura 11.** Boletines recomendados para resolver vulnerabilidades.

Observando detalles de las vulnerabilidades y el modo de solución, se detecta que Microsoft propone parches por cada vulnerabilidad para los sistemas operativos vigentes a la fecha y no considera los obsoletos como Windows XP y Windows Server 2003. El detalle de los boletines recomendados se observan en la Figura 12.

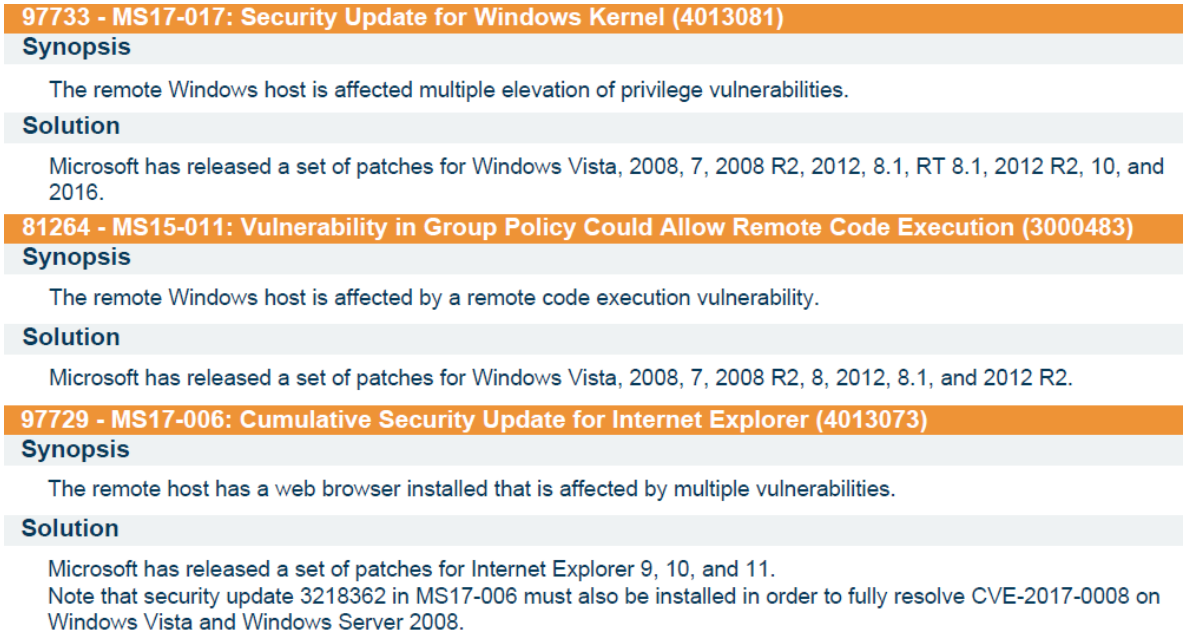



**Figura 12.** Detalles de boletines de seguridad recomendados.

Por otro lado, de acuerdo a estadísticas mundiales (Referirse a sección 2.2.2) existe una gran cantidad de servidores que no tienen activado el servicio de actualizaciones automáticas, no tienen conexión directa a internet o no se realizan las instalaciones completas de actualizaciones y parches por no contar con un proceso de seguridad definido.

Para los casos en que los servidores tiene activado el servicio de actualizaciones automáticas, la distribución e instalación de parches es realizado de manera manual por un administrador del servidor, quién debe individualmente por cada servidor verificar si existen actualizaciones o parches, y en ese caso, descargarlos e instalarlos manualmente. El procedimiento es lento e ineficiente, ya que el administrador debe ingresar a cada servidor para verificar la existencia de algún parche y debe descargar en cada servidor los parches correspondientes, repitiendo el procedimiento en cada servidor, posiblemente realizando múltiples descargas del mismo parche o actualización. Además, no se identifican las vulnerabilidades que tienen los servidores, por lo que se van a mitigar únicamente las que están asociadas a parches que reconoce automáticamente el sistema operativo.

## 5.4. Modelo de Seguridad

Al momento del ataque mundial de las dos variantes de Ransomware, tanto de WannaCry como de Petya durante 2017, el modelo de seguridad propuesto en este trabajo de tesis estaba siendo aplicado en la organización *Enterprise S.A.*, aunque no completamente maduro. Los puntos importantes definidos como: roles de usuarios, documentos primordiales y el modelo de proceso completo ya se estaba aplicando. Si bien todavía no estaban definidos los indicadores del modelo de madurez y métricas de comparación, se considera que los resultados de la evaluación de vulnerabilidades es confiable y su aplicación como un caso de éxito.

**Roles de usuario**

La gestión de vulnerabilidades de servidores en Nube privada se llevó a cabo con dos actores involucrados en la ejecución de las tareas: un especialista en la operación perteneciente al área Seguridad Informática y un operador de Infraestructura. Estas dos personas, pertenecientes a dos áreas diferentes, ejecutaron el total de las tareas requeridas.

**Documentación**

En cuanto a la documentación del modelo de seguridad, durante el caso analizado se trabajaron con los siguientes:

- Documento de Política donde se definen los usuarios involucrados, dos documentos requeridos y el plan de acción para afrontar riesgos de seguridad.
- Documento de Procedimiento donde se detalla el flujo de tareas para obtener y verificar actualizaciones y parches de seguridad.
- Documento Instructivo para actualizar base de firmas en herramienta de análisis de vulnerabilidades Nessus.

- Documento Instructivo para actualizar base de firmas en herramienta de análisis de vulnerabilidades MBSA.
- Documento Instructivo para descargar e instalar actualizaciones y parches en servidores de Nube privada, mediante la herramienta WSUS.
- Documento Planilla de parches y actualizaciones utilizado para realizar e indicar el plan de actualizaciones, utilizado para liberar e instalar los parches y actualizaciones indicadas en el mismo.

**Modelo de Proceso**

En la organización se ejecuta el proceso de seguridad mensualmente, el segundo martes del mes, lo que permite tener actualizada la base de vulnerabilidades y mitigaciones con respecto a la publicación planificada de boletines de Microsoft. Se trabaja con herramientas que permiten automatizar: descubrimiento de activos, análisis de vulnerabilidades, obtención e instalación de parches y actualizaciones. Además, de manera manual se realiza: actualización de base de firmas de la herramienta de análisis de vulnerabilidades, análisis de parches y actualizaciones a liberar, y reinicio de servidores para finalizar la instalación de los mismos.

Las herramientas de seguridad utilizadas en la aplicación del modelo de seguridad, fueron tres específicas. Para el análisis de vulnerabilidades y detección de actualizaciones y parches a instalar se trabajó con dos: Tenable Nessus y Microsoft Baseline Security Analyzer (MBSA). Por otro lado, se utilizó la herramienta automatizada Windows Server Update Services (WSUS) para la descarga, distribución e instalación de parches y actualizaciones.

La organización considera que el proceso de seguridad se debe aplicar al menos a todos los servidores en Nube privada considerados críticos, lo cual representan el 50% del total de servidores de la infraestructura de la organización. Además, se selecciona un servidor en particular considerado no crítico para realizar las pruebas de funcionamiento de parches y actualizaciones. De este modo se inicia la fase 1 "Identificación", donde se utiliza

una herramienta automatizada que realiza descubrimiento de activos como es el caso de servidores en Nube privada, mediante análisis de red, consulta al controlador de dominio y por rango IP, como se observa en la Figura 13.

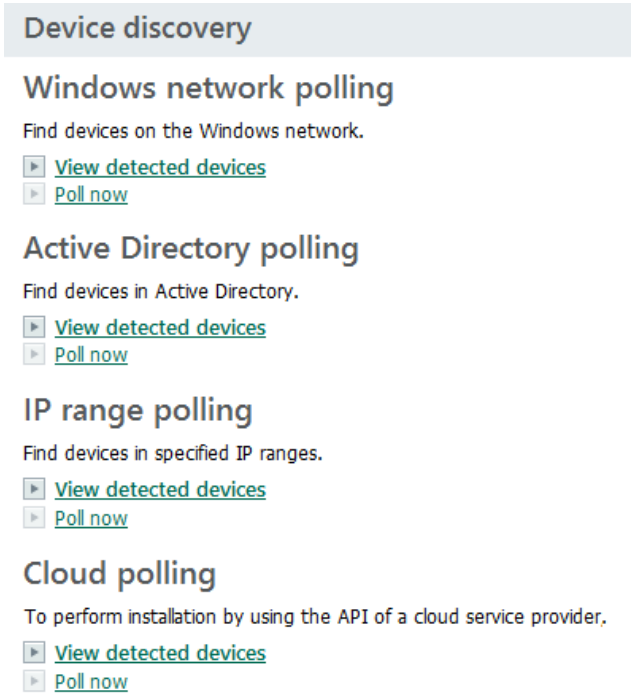



**Figura 13.** Descubrimiento automatizado de activos.

En la fase 2 "Disponibilidad", se actualizó la base de firmas de seguridad y se ejecutó el análisis de vulnerabilidades sobre un porcentaje de los activos identificados al inicio con las dos herramientas de seguridad: Tenable Nessus y Microsoft Baseline Security Analyzer, con el objetivo de hallar vulnerabilidades y exploit en cada una. El análisis se planificó de manera nocturna en los momentos de menor carga de trabajo. En la Figura 14 se revisa que la ejecución de la tarea se haya realizado de manera correcta en todos los servidores en Nube privada de la infraestructura.

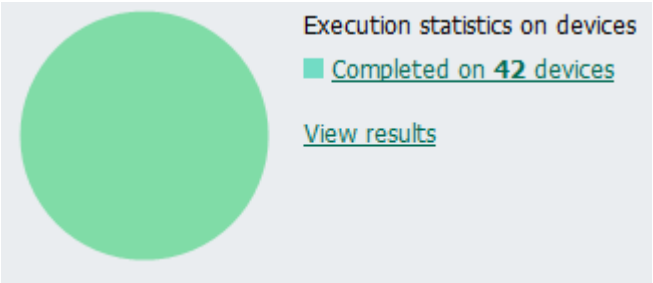


**Figura 14.** Ejecución de VA en todos los servidores de la infraestructura.

Como resultado se obtuvo información detallada sobre vulnerabilidades a mitigar y parches de corrección. Información general de un caso de reporte se observa en la Figura 15, donde el escaneo se hizo el jueves 16 de marzo de 2017 a las 02:20 hs.

**Scan Information**

| | |
|---|---|
| Start time: | Thu Mar 16 02:20:56 2017 |
| End time: | Thu Mar 16 02:41:18 2017 |

**Results Summary**

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 3 | 7 | 2 | 1 | 215 | 228 |

**Figura 15.** Resultado de análisis de vulnerabilidades.

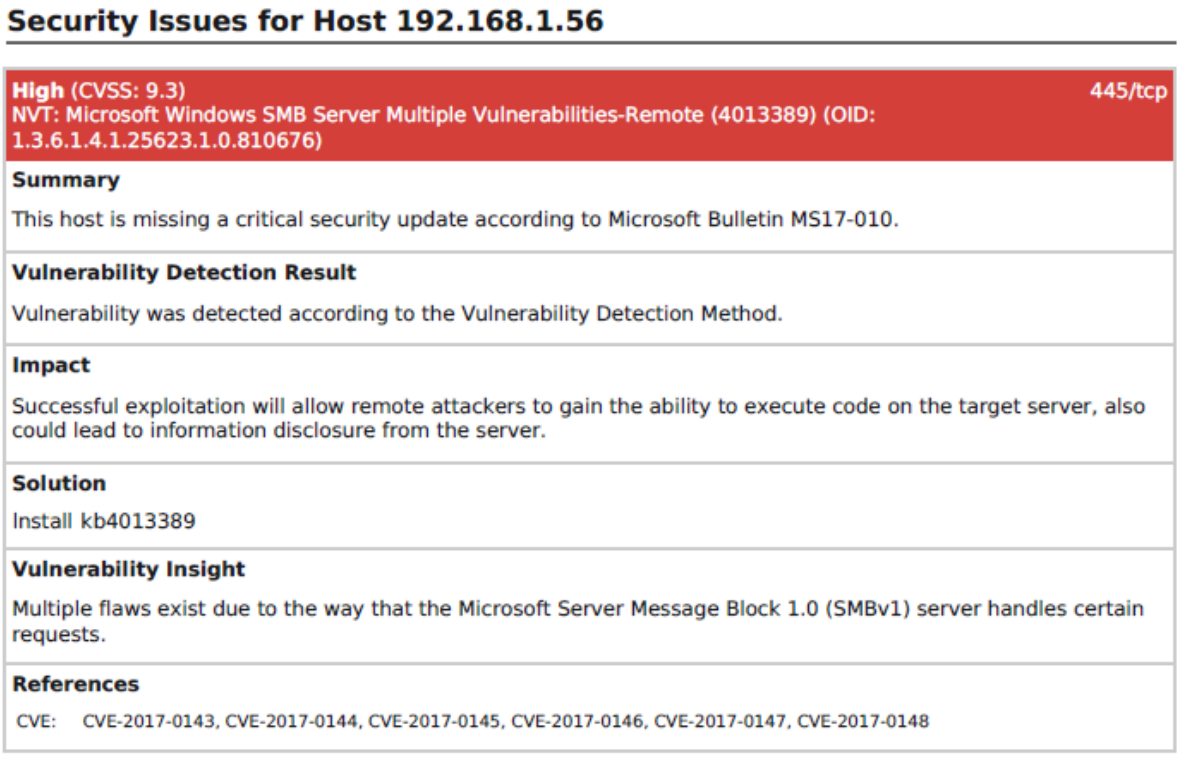
A diferencia de la herramienta de actualizaciones automáticas que propone Microsoft, el análisis de vulnerabilidades experto detecta mayor cantidad de vulnerabilidades y no sólo asociadas al sistema operativo Microsoft, sino vulnerabilidades por canal seguro, cifrado y malas prácticas implementadas, entre otras cuestiones. En la Figura 16, se observan algunas de las vulnerabilidades detectadas en el escaneo del 16 de marzo de 2017, donde se detecta la vulnerabilidad de SMB considerando criticidad Alta (High).

| Severity | Description | CVSS | Count |
|---|---|---|---|
| High | Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) | 9.3 | 1 |
| Medium | DCE/RPC and MSRPC Services Enumeration Reporting | 5.0 | 1 |
| Medium | SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 5.0 | 1 |
| Medium | SSL/TLS: Report Weak Cipher Suites | 4.3 | 4 |
| Low | TCP timestamps | 2.6 | 1 |

**Figura 16.** Vulnerabilidades detectadas con la herramienta Tenable Nessus.

Además de detectar las vulnerabilidades de cada servidor en Nube privada, la herramienta de análisis de vulnerabilidades indica por cada una, los métodos para mitigar o eliminar la misma. En la Figura 17 se observa el detalle de la vulnerabilidad asociada al

protocolo SMB de Microsoft publicada en el boletín MS17-010, su impacto y el método de mitigación o modo de solución.



**Security Issues for Host 192.168.1.56**

**High** (CVSS: 9.3) — 445/tcp
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)

**Summary**

This host is missing a critical security update according to Microsoft Bulletin MS17-010.

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**

Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

**Solution**

Install kb4013389

**Vulnerability Insight**

Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

**References**

CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148

**Figura 17.** Detalle de vulnerabilidad publicada en MS17-010.

La fase 3 "Aplicabilidad" inicia a partir de la información relevada de los reportes de análisis de vulnerabilidades generados por las dos herramientas de análisis utilizados, el operador de seguridad arma el documento con el plan de actualizaciones considerando los parches y actualizaciones de seguridad que se utilizarán para mitigar las vulnerabilidades detectadas. Se observa en la Tabla 12 la carátula del documento de plan de actualizaciones y en la Tabla 13 se presenta el listado de parches correspondiente a dicho plan.

| *Nombre del Documento*<br>Plan de actualizaciones | | | |
|---|---|---|---|
| **Nombre del Documento** | | | |
| **Historial de Revisiones** | | | |

| Fecha | Versión | Descripción | Autor | |
|---|---|---|---|---|
| 16/03/2017 | 1.0 | Generación de documento | Simón Cifre | |
| | | | | |
| **Índice** | | | | |
| Carátula | 1 | | | |
| Plan de act. | 2 | | | |
| | | | | |
| **Definiciones y Glosario** | | | | |
| KB | Knowledge Base. | | | |
| | | | | |
| **Propósito del documento** | | | | |
| El presente documento tiene por objetivo presentar el plan de actualizaciones de parches a liberar e instalar, correspondiente al mes de marzo de 2017. | | | | |
| | | | | |

**Tabla 12.** Carátula documento de Plan de actualizaciones.

| Orden | CVE | KB | Sistema Operativo | Vulnerabilidad resuelta |
|---|---|---|---|---|
| 1 | CVE-2017-0143 | KB4013389 | Windows Server 2008<br>Windows Server 2012 | SI |

| | | | | |
|---|---|---|---|---|
| 2 | CVE-2017-0008 | KB4012204 | Windows Server 2008<br>Windows Server 2012 | SI |
| 3 | CVE-2017-0023 | KB4012214 | Windows Server 2012 | SI |
| 4 | CVE-2017-0143 | KB4012598 | Windows Server 2008<br>Windows Server 2012 | SI |

**Tabla 13.** Cuerpo documento de Plan de actualizaciones.

En la fase 4 "Adquisición", utilizando la herramienta automatizada de descarga, distribución e instalación de parches y actualizaciones, el operador de infraestructura libera el parche KB4013389 que de acuerdo a la herramienta de análisis de vulnerabilidades, presenta la solución a la vulnerabilidad de protocolo SMB publicado en el boletín MS17-010. En Figura 18 se observa un panel de la herramienta donde se selecciona el parche para ser instalado en los servidores de Nube privada.

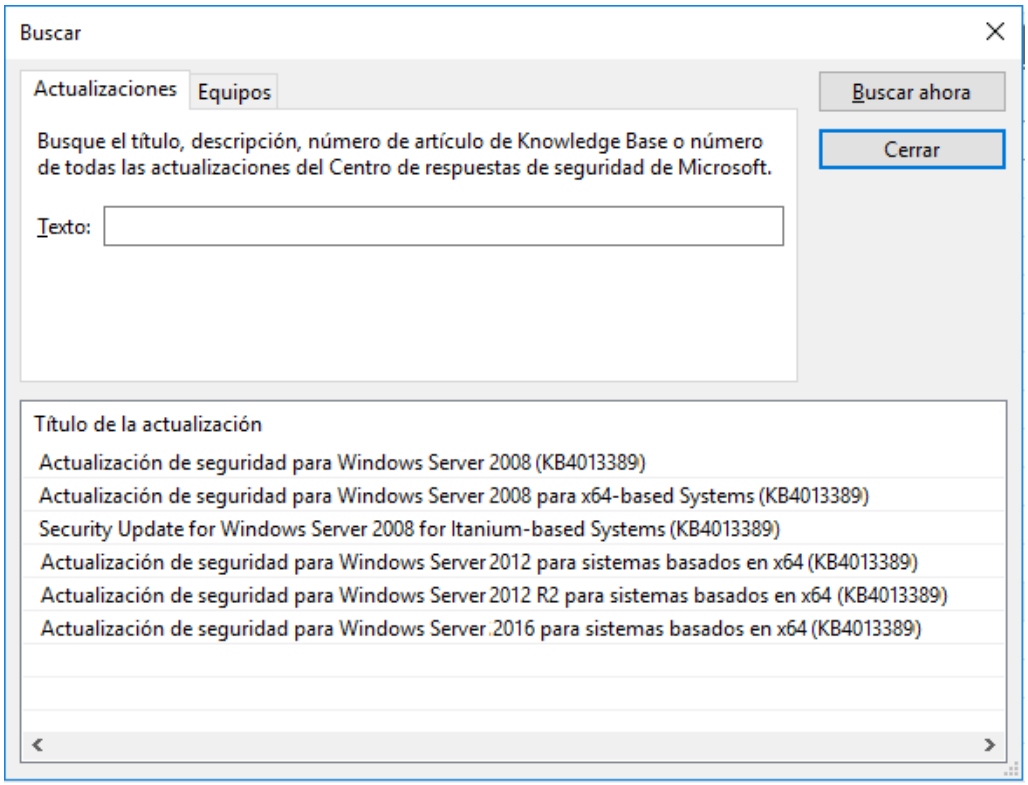



**Figura 18.** Selección de parche para liberar a servidores en Nube privada.

En la fase 5 "Validación", se trabaja con un único servidor en Nube privada que fue considerado dentro de los no críticos para realizar la validación de los parches y actualizaciones liberadas. Aquí se realiza la instalación de los mismos, de acuerdo al plan de actualizaciones y se reinicia. Este servidor es testeado por 24 horas por operadores de infraestructura verificando su correcto funcionamiento. Posterior a este lapso y al no haberse encontrado fallas o errores, se prosigue con el proceso.

La fase 6 "Despliegue" se realiza la liberación e instalación de parches en cada uno de los servidores en Nube privada, los mismos deben ser reiniciados para que finalice la instalación y se realice la configuración del mismo. Se consideran rangos horarios nocturnos para el reinicio de los servidores para que no afecte la operación diaria y genere bajo impacto. En la Figura 19 se observa momento de reinicio de servidor donde se aplica la configuración del parche finalizando su instalación.


**Figura 19.** Selección de parche para liberar a servidores en Nube privada.

Al momento que el servidor inició con el parche instalado, se asegura que se mitigó la vulnerabilidad indicada en el boletín MS17-010.

**Indicadores de vulnerabilidades**

A continuación se calculan los indicadores aplicados a la organización del caso de estudio.

- Frecuencia de escaneo: Bajo (escaneo mensual).
- Intensidad de escaneo: Moderado (dos escaneos diferentes).
- Cobertura de autenticación: Moderado (solo activos críticos con credenciales de autenticación).
- Cobertura de activos: Moderado (se analizan los servidores en Nube privada considerados críticos dentro de la infraestructura).
- Cobertura de vulnerabilidades: Moderado (herramientas con 50% de complementos de vulnerabilidades disponibles).

**Modelo de madurez**

A partir de los indicadores de rendimiento de la evaluación de vulnerabilidades, se calcula el nivel de madurez de la organización el cual proporciona una capa en la base para una mejora continua del proceso en la organización y se mide por el logro en el cumplimiento de los indicadores de rendimiento. El nivel calculado para la organización del caso de estudio es "Nivel 1: Madurez baja". Si bien el modelo de seguridad implementado tiene indicadores de vulnerabilidades con resultados más optimistas, la frecuencia de escaneo es el indicador que disminuye la madurez, generando un resultado bajo.

Un modelo de seguridad con madurez baja como la presentada cumple con los requisitos esenciales de seguridad de la información requeridos y recomendados por los estándares internacionales. Esto se asocia principalmente con el hecho de tener definido un proceso de gestión de vulnerabilidades para el aseguramiento de activos de la organización, con roles de usuarios definidos y toda documentación correspondiente. La problemática de este modelo se centra en la incapacidad que tiene la organización de hacer frente a parches y actualizaciones de emergencia, publicados fuera de término y que el modelo tiene que esperar un mes completo para que se detecte su vulnerabilidad y se aplique el parche que mitiga la misma. Además, no satisface la seguridad de la información de manera completa ya que solo realiza el proceso en el 50% de sus activos.

La recomendación principal a aplicar para mejorar la madurez de la organización en cuanto a gestión de vulnerabilidades es aumentar la frecuencia de escaneo de servidores en Nube privada. Si esta frecuencia pasa de ser mensual a semanal, no solamente se logrará el Nivel 2, sino que teniendo en cuenta el buen estado del resto de los indicadores calculados, la organización podrá lograr el nivel 3: Madurez media a alta".

Como recomendaciones adicionales, solo para lograr alcanzar el nivel de madurez superior (Nivel 4: Madurez Alta), las consideraciones son:

- Ampliar la cobertura de análisis de vulnerabilidades a todos los servidores en Nube privada.
- Ampliar el uso de credenciales para el escaneo autenticado a fin de lograr una visión más profunda y confiable de las vulnerabilidades de un activo.
- Aprovechar las plantillas de escaneo personalizadas que se centran en familias tecnológicas específicas y para casos de uso específicos, como las vulnerabilidades aprovechables.
- Comenzar a aprovechar el escaneo distribuido para equilibrar las evaluaciones en varios escáneres y para reducir la duración del escaneo.

## 5.5. Observaciones

Mensualmente Microsoft publica boletines de seguridad donde detalla vulnerabilidades propias y parches de correcciones a las mismas. Si bien se brindan las mitigaciones correspondientes para cada caso, si las organizaciones no las aplican, son públicas las vulnerabilidades por lo que los atacantes pueden explotar las mismas generando un ataque informático.

Las organizaciones que no tienen un modelo de seguridad para la gestión de vulnerabilidades, son constantemente blancos de ataques. Esto ocurrió en Mayo y Junio de 2017 donde se ejecutaron ataques masivos con dos variantes de Ransomware que afectaron cientos de miles de servidores en la nube, a partir de una vulnerabilidad publicada por Microsoft en Marzo del mismo año. Los afectados a dichos ataques expresaron su falta de

accionar interno sobre cuestiones de gestión de vulnerabilidades.

En el caso de la implementación presentada anteriormente, se demuestra la efectividad del proceso de seguridad que permitió mitigar rápidamente las vulnerabilidades publicadas por Microsoft, actuando para lograr que la organización no fuera víctima de las variantes de Ransomware. Además, se destaca que dicha organización no requirió tener herramientas automatizadas completamente ni un modelo de seguridad con alto nivel de madurez para que el mismo sea efectivo. Por otro lado, el proceso definido permite agilizar el flujo de tareas reduciendo los tiempos de operación respecto a los casos en los que no hay un modelo de seguridad con un procedimiento definido.

## 6. Conclusiones

Cada año son más las organizaciones que confían en la Nube para sus datos. Gran parte de las cargas de trabajo empresariales ya se están ejecutando en la Nube y se estima que seguirá en aumento. La seguridad es uno de los principales problemas de sistemas de información basados en la Computación en la Nube. Los vectores de ataques son las vulnerabilidades y su conexión en una red de redes incrementa la exposición a ataques de hackers.

Los estándares internacionales de seguridad de la información como O-ISM3 e ISO27000 presentan lineamientos y buenas prácticas a seguir para lograr seguridad de la información eficiente en las organizaciones, pero debido a sus limitaciones de implementación, no resulta sencilla llevarlo a cabo directamente en la operación.

Teniendo en cuenta la posibilidad de manejar datos sensibles como así también la problemática de seguridad asociada a las vulnerabilidades, la implementación de Computación en la Nube debe llevarse a cabo a partir de un modelo de seguridad basado en estándares de seguridad que permita garantizar su buen uso y privacidad.

Implementar un modelo de seguridad basado en la gestión de vulnerabilidades de servidores en Nubes privadas, permite definir un proceso completo y eficiente de gestión de

vulnerabilidades compuesto por lineamientos de una política de seguridad y un proceso de seguridad detallado, lo que brindará protección a las Nubes privadas de las organizaciones.

La política de seguridad apoyada en estándares internacionales como O-ISM3 e ISO27000, logra normalizar los roles de usuarios con asignación y permisos específicos para cada tarea, documentación requerida con formatos estandarizados y cumplimientos puntuales, y métricas con indicadores para establecer controles, medir el desempeño y aplicar mejora continua.

El modelo de proceso de seguridad propuesto establece un procedimiento específico para la gestión de vulnerabilidades donde por cada rol de usuario se definen las tareas operativas a realizar y los documentos requeridos a generar. Seguir paso a paso el procedimiento permite no solo el aseguramiento frente a vulnerabilidades de los servidores en Nube privada, sino cumplimentar con los requisitos de los estándares internacionales de seguridad. Por otro lado, la representación gráfica del proceso mediante la técnica de notación Business Process Model and Notation (BPMN), permite que sea intuitivo y de fácil visualización para usuarios técnicos como para usuarios de negocios.

En cuanto a las métricas de control, se proponen indicadores de rendimiento para la evaluación de vulnerabilidades y se corresponden con la madurez del procedimiento. Los niveles de madurez proporcionan una capa en la base para una mejora continua del proceso en la organización y se miden por el logro en el cumplimiento de los indicadores de rendimiento. Además, las buenas prácticas propuestas como recomendaciones permiten mejorar los indicadores de rendimiento y con esto, el nivel de madurez de la organización en cuanto al proceso de aseguramiento de servidores en Nube privada.

A partir de las características y ventajas presentadas, el modelo de seguridad propuesto se adapta completamente a los estándares internacionales más importantes como ISO/IEC 27001 y O-ISM3. En particular, a ISO/IEC 27001, que es la norma de seguridad de uso generalizado para todas las organizaciones a nivel mundial, y al estar implementado mediante el Estándar O-ISM3, se tienen definidos todos los procesos operativos a realizar. Si bien el modelo de seguridad propuesto puede generar dificultad de aceptación para su implementación en algunas organizaciones, fundamentalmente debido a un cambio de

paradigmas en el pensamiento de los usuarios en cuanto a la manera de trabajar y de organizar sus tareas, se obtiene un modelo que otorga una mejora de la imagen empresarial ante los propios empleados y clientes dado que les transmite confianza sobre la protección de los datos depositados en la misma, generando una diferenciación frente a sus competidores y mayores oportunidades de negocio. Además, permite que los operadores puedan realizar sus tareas de manera más ágil, organizada y optimizada, reduciendo los costos, tiempos y amenazas posibles.

El modelo de seguridad propuesto es transversal a todas las capas de servidores en Nube privada y que por lo tanto, permite asegurar las vulnerabilidades a nivel operativo, de servicios, y de aplicaciones y software. El modelo es capaz de adaptarse completamente a cualquier organización independientemente de su tamaño, el contexto y los recursos. Al proveer niveles incrementales de madurez con recomendaciones explícitas, facilita una forma de tener resultados concretos en poco tiempo.

Por otro lado, el modelo contribuye oportunamente para la creación de un SGSI alineado con la misión de la organización, el cumplimiento de sus necesidades, y la priorización y optimización de las inversiones en seguridad de la información, midiendo el desempeño mediante la aplicación de métricas.

## 7. Trabajo Futuro

Con la finalización de la presente tesis de maestría, se vislumbran nuevos proyectos e investigaciones futuras. La primer consideración de trabajo futuro está asociado con completar los requerimientos de ISO/IEC 27001 con todos los procesos operacionales de O-ISM3 asociados a "OSP-5 Actualizaciones de Seguridad", lo que incluye: Gestión de inventario de activos de información (OSP-3), Gestión de cambios (OSP-4) y Medidas de seguridad de control de cambios (OSP-9).

Por otro lado, se considera la opción de agregar al modelo de seguridad para gestión de vulnerabilidades de servidores en Nubes privadas los niveles estratégicos y tácticos que propone O-ISM3, lo que permitirá proporcionar la infraestructura para la implementación,

evaluación y mejora de los procesos, como así también la minimización de riesgos.

Como tercera consideración de trabajo futuro se considera un proyecto que involucre el uso de ontologías que permitan automatizar la gestión de la documentación.

## 8. Bibliografía

[1] Aller, C. F. (2012). Algunos retos de la protección de datos en la sociedad del conocimiento: especial detenimiento en la computación en nube (cloud computing). Revista de Derecho de la UNED (RDUNED), (10).

[2] Flantrmsky-Cárdenas, H. H. (2012). La Computación en Nube y el cambio del Universo Informático. Pensamiento y Cultura, 15(1), 88-93.

[3] Tenable (2019). Informe de inteligencia de vulnerabilidades.4-20.

[4] Castro, I. (2019). Seguridad en la nube, tips y tendencias. Publicado por CeroUno.

[5] Bond, D. (2018). Los 'hackers', a por las plataformas en la nube. Revista Expansión.

[6] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 1(1), 7-18.

[7] AKAMAI (2019). CDN & Cloud Services Glossary: Vulnerability Management.

[8] Tu, C. Z., Yuan, Y., Archer, N., & Connelly, C. E. (2018). Strategic value alignment for information security management: a critical success factor analysis. Information & Computer Security, 26(2), 150-170.

[9] ISO 27000 – EL PORTAL DE ISO EN ESPAÑOL (2013). ISO 27000. Disponible en: http://www.iso27000.es/iso27000.html. Fecha de consulta: 22/03/2019.

[10] THE OPEN GROUP (2011). Open Information Security Management Maturity Model (O-ISM3). Van Haren Publishing.

[11] Jara, H (2017). Introducción a la Gestión de Vulnerabilidades. Entropy Security.

[12] Windows Server Update Services – Microsoft (2019). Disponible en: https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus. Fecha de consulta: 17/04/2019.

[13] Software Delivery – Akamai (2019). Disponible en: https://www.akamai.com/es/es/resources/software-delivery.jsp. Fecha de consulta: 18/04/2019.

[14] Patch Management Security – Kace (2019). Disponible en: https://www.quest.com/mx-es/products/kace-systems-management-appliance/patch-management-security.aspx. Fecha de consulta: 17/04/2019.

[15] Jouini, M., & Rabai, L. B. A. (2019). A security framework for secure cloud computing environments. In Cloud Security: Concepts, Methodologies, Tools, and Applications (pp. 249-263). IGI Global.

[16] Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: implementation, management, and security. CRC press.

[17] Haber, M. J., & Hibbert, B. (2018). Vulnerability Management Design. In Asset Attack Vectors (pp. 119-123). Apress, Berkeley, CA.

[18] Poonia, A. S., Banerjee, C., Banerjee, A., & Sharma, S. K. (2018). Vulnerability identification and misuse case classification framework. In Soft Computing: Theories and Applications (pp. 659-666). Springer, Singapore.

[19] Krutz, R. L., & Vines, R. D. (2010). Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing.

[20] Cifre, S. (2018) Marco de trabajo estructurado para la seguridad de la información en servidores basado en estándares internacionales. Publicado como trabajo final de integración en carrera de posgrado Especialización en Ingeniería en Sistemas de Información - UTN Facultad Regional Santa Fe.

[21] Cifre, S., Roa, J. (2019) Gestión y operación de seguridad en servidores Web basadas en ISO/IEC27000 y O-ISM3. 48 JAIIO - Jornadas Argentinas de Informática. IETF Day

2019 - Taller del Grupo de Trabajo de Ingeniería de Internet/Argentina.

[22] Garcia, I. (2018). Server definition and types.

[23] Nasser, C., Cuesta, D., Fairhust, N. (2012). Tipos de servidores. Publicado en Claranet.

[24] Virguez, M. A. (2016). Los 19 tipos de servidores principales. Publicado en Lifeder.

[25] Martinez Godínez, F., Gutierrez Galán, B. (2017). Cómputo en nube. Ventajas y desventajas. Publicado por revista DGTIC Seguridad. Universidad Nacional Autónoma de México.

[26] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[27] Hewlett Packard Enterprise (2018). ¿Qué es computación en la nube? Publicado en: https://www.hpe.com/lamerica/es/what-is/cloud-computing.html. Fecha de consulta: 19/05/2019.

[28] Ruiz Rodríguez, E. (2012). Cinco problemas que impiden que las empresas adopten el Cloud Computing. Revista Cloud Computing.

[29] INCIBE - INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA (2017). Amenaza vs Vulnerabilidad, en qué se diferencia.

[30] CVE (2019). Common Vulnerabilities and Exposures. Publicado en: https://cve.mitre.org/. Fecha de consulta: 25/05/2019.

[31] Guillermo, Graciela (2018). Vulnerabilidades informáticas. Publicado en revista Tecnología Informática.

[32] Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, 144-166.

[33] Ganacharya, T. (2017). WannaCrypt ransomware worm targets out-of-date systems. Publicado por Microsoft Security.

[34] Canella, C., Van Bulck, J., Schwarz, M., Lipp, M., Von Berg, B. Ortner, P., Piessens,

F., Evtyushkin, D., Gruss, D. (2019). A Systematic Evaluation of Transient Execution Attacks and Defenses. Graz University of Technology, imec-DistriNet, KU Leuven, College of William and Mary.

[35] Algar, P. (2017). Ataque Ransomware: Microsoft lanza un parche de seguridad para Windows. Publicado por Microsoft.

[36] Huatala, L (2018). Spectre y Meltdown: lo que debes saber de los fallos de chips Intel, AMD y ARM. Publicado por CNET en Español.

[37] Quijije, J (2017). Aumento de ataques de malware de minería.

[38] Hernandez, A. (2018). Ataques hacker en smartphones por bitcoins.

[39] https://docs.oracle.com/cd/E24842_01/html/E23289/swmgrpatchtasks-1.html

[40] INCIBE - INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA (2018). Gestión de parches en sistemas de control.

[41] SYMANTEC SECURITY (2018). IT management suite.

[42] ISO 27002 – EL PORTAL DE ISO EN ESPAÑOL (2013). Control de las vulnerabilidades técnicas. Disponible en: http://www.iso27000.es/iso27000.html. Fecha de consulta: 22/03/2019.

[43] Yesid Avila, F. (2018). Escaner de vulnerabilidades. Publicado en Security Hack Labs.

[44] Myerson, J. (2015). Cuatro herramientas de pen testing para mejorar la seguridad empresarial. Publicado en Search Data Center.

[45] Microsoft Baseline Security Analizer – Microsoft (2019). Disponible en: https://www.glosarioit.com/MBSA. Fecha de consulta: 18/04/2019.

[46] Nessus Vulnerability Scanner – Tenable (2019). Disponible en: http://www.tenable.com/products/nessus-vulnerability-scanner. Fecha de consulta: 11/05/2019.

[47] Windows Server Update Services – Microsoft. Disponible en:

https://technet.microsoft.com/es-es/windowsserver/bb332157.aspx. Fecha de consulta: 07/05/2019.

[48] CFengine (2019). Disponible en: https://cfengine.com/. Fecha de consulta: 11/05/2019.

[49] Eliécer, J. (2019). Virtual patching. Publishing by B-Secure.

[50] MAX DE GORBITZ (2018). Evolución en modelos y marcos de gestión de la seguridad de la información y la ciberseguridad. Congreso y Feria Iberoamericana de Seguridad de la Información - Segurinfo 2018.

[51] ISO TOOLS EXCELLENCE (2016). ¿Por qué las organizaciones necesitan certificar la ISO 27001? Publicado por Excellence Chile.

[52] THE OPEN GROUP (2011). Open Information Security Management Maturity Model (O-ISM3). Van Haren Publishing.

[53] INCIBE - INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA. Gestión de parches. Fecha de consulta: 17/03/2018.

[54] Nyanchama, M. (2015). Enterprise Vulnerability Management and Its Role in Information Security Management. Information Systems Security, 14(3), 29-56.

[55] INCIBE - INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA (2017). Boletines de seguridad de Microsoft de marzo de 2017. Fecha de consulta: 23/03/2019.

[56] MICROSOFT (2017). Microsoft Security Bulletin MS17-010 – Critical. Publicado en Microsoft Security Bulletins.

[57] JOSE MANUEL POVEDA (2011). Los activos de seguridad de la información. Sección 7. Publicado en UNI - RUACS.

[58] C. PARDO, F. PINO, F. GARCIA, M. PIATTINI, M. BALDASSARRE (2009). A process for Driving the Harmonization of Models. Publicado en 11th International Conference on Product Focused Software Development and Process Improvement - Limerick, Irlanda.

[59] ECURED (2015). Seguridad en los servidores. Disponible en: http://www.ecured.cu/Seguridad_en_los_servidores. Fecha de consulta: 24/02/2018.

[60] INCIBE - INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA. Amenaza vs Vulnerabilidad. Fecha de consulta: 24/02/2018.

[61] INCIBE - INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA. Parches. Fecha de consulta: 24/02/2018.

[62] Chen, Q., & Bridges, R. A. (2017). Automated behavioral analysis of malware: A case study of wannacry ransomware. In 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 454-460). IEEE.

[63] González, G. (2016). La criptomoneda y el mercado digital (Doctoral dissertation, Tesis para obtención del grado de Maestro en Ciencias Económicas, Instituto Politécnico Nacional, Ciudad de México, México).

[64] Dan Van, B. (2016). Por qué BPMN. Origen y razones para su adopción. Publicado en Global Logic Club.

[65] Booch, G., Rumbaugh, J., Jacobson, I., Martínez, J. S., & Molina, J. J. G. (2009). El lenguaje unificado de modelado (Vol. 1). Madrid: Addison wesley.

[66] Tabares, M. S., Pineda, J. D., & Barrera, A. F. (2008). Un patrón de interacción entre diagramas de actividades UML y sistemas workflow. Revista EIA, (10), 105-120.

[67] White, S. A. (2008). BPMN modeling and reference guide: understanding and using BPMN. Future Strategies Inc.

[68] Soto, D (2016). Qué es BPMN y para que sirve. Publicado por Nextech Education Center.

[69] Silver, Bruce (2011). BPMN Method & Style with BPMN Implementer's Guide, 2do Edition, Cody-Cassidy Press, Aptos, USA.

# Anexo I – Definiciones

**TI:** Tecnología de la información. Es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras organizaciones. Engloba todo lo relacionado con la informática, la electrónica y las telecomunicaciones [57].

**Proceso:** Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados [58].

**Activo de información:** Elemento que contiene o manipula información: equipos informáticos, equipos de comunicaciones, servicios informáticos y de comunicaciones, software de sistema, ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, utilidades generales y personas. Estos últimos son los que en última instancia generan, transmiten y destruyen información, es decir, dentro de una organización se han de considerar todos los tipos de activos de información [57].

**Servidor:** Un servidor es una computadora (física o virtual) que, formando parte de una red, provee servicios a otras computadoras denominadas clientes. Existe una gran variedad de servidores que desarrollan variadas funciones, entre los que podemos destacar: Servidor Web, Servidor de correo, Servidor de base de datos, Servidor Proxy, Servidor de archivos, Servidor de impresiones, y Servidor de telefonía [59].

**Vulnerabilidad:** Errores que permiten realizar desde afuera actos sin permiso del administrador del equipo, incluso se puede suplantar al usuario. Estos permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo [60].

**Gestión de vulnerabilidades:** La gestión de vulnerabilidades es un proceso continuo de TI consistente en la identificación, evaluación y corrección de vulnerabilidades en los sistemas de información y las aplicaciones de una organización. Va más allá de la evaluación de las vulnerabilidades, ya que categoriza los activos y clasifica las vulnerabilidades según el nivel de riesgo. La gestión de vulnerabilidades ofrece a las organizaciones un medio rentable para proteger las infraestructuras de TI fundamentales frente a las lagunas de

seguridad [7].

**Parche:** Un parche es una pieza de software diseñado para actualizar un programa de computadora o sus datos de apoyo, para corregir o mejorar la misma. Esto incluye la fijación de las vulnerabilidades de seguridad y otros aspectos. Con este tipo de parches, generalmente llamados correcciones de errores, permite mejorar la facilidad de uso o el rendimiento [61].

**CVE:** Diccionario cuyo propósito es propiciar la distribución de datos en bases de datos de vulnerabilidades y herramientas de seguridad separadas. Comprende una lista de nombres estandarizados lo que facilita la búsqueda y asignación [30].

**Malware:** Software malicioso que tiene como objetivo infiltrarse o dañar un sistema de información sin el consentimiento de su propietario. Se destacan virus, gusanos, troyanos, keyloggers, botnets, spyware, adware y ransomware [62].

**Ransomware:** Tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos [62].

**Criptogusano:** Malware del tipo gusano que utiliza criptografía para cifrar archivos y así bloquear el acceso a los mismos a los usuarios válidos. Un caso de criptogusano es el Ransomware [62].

**Criptomoneda:** Medio digital de intercambio que utiliza criptografía fuerte para asegurar las transacciones controlar la creación de unidades adicionales y verificar la transferencia de activos. Las criptomonedas son un tipo de divisa alternativa y de moneda digital [63].

# Anexo II – Modelado

Se requiere una notación unificada, eficaz y simple que sirva como medio de comunicación entre todos los actores involucrados en los procesos de seguridad. Los métodos comunes presentan diversos problemas como: necesidad de traducir los requerimientos entre áreas y sectores, errores en la comunicación y traslado de directivas, falta de eficiencia en la realización de tareas y actividades, escaso control del avance de los procesos organizaciones. Dichos problemas implican menor productividad, y un mal aprovechamiento de recursos, tiempo y dinero [64].

Generalmente las organizaciones atacan parcialmente estos problemas de una manera "ad-hoc", introduciendo algún esquema interno de comunicación. Pero muchas veces, en organizaciones grandes, tales esquemas varían entre los distintos sectores, lo cual sigue generando confusión. Incluso cuando se genera un mismo esquema para un determinado proceso, a lo largo de la organización, el mismo puede ser desconocido tanto por los mismos empleados que debían aplicarlo, como por terceras partes, lo cual afectaba negativamente tanto la productividad de dichos empleados, como la interacción con otras organizaciones y proveedores de servicios [64].

En base a la problemática, se analizan diferentes lenguajes de modelado de procesos para definir uno que cumpla con las expectativas planteadas. Entre estos lenguajes se destacan dos: Diagrama de actividades UML y BPMN.

## 1. Diagrama de actividades UML

El Diagrama de Actividad es un diagrama de flujo del proceso multi-propósito que se usa para modelar comportamiento, casos de uso, o una clase, o un método complicado. También se suele utilizar para modelar procesos. Un diagrama de actividad es parecido a un diagrama de flujo; la diferencia clave es que los diagramas de actividad pueden mostrar procesado paralelo. Esto es importante cuando se usan diagramas de actividad para modelar procesos de negocio, algunos de los cuales pueden actuar en paralelo, y para modelar varios hilos en los programas concurrentes [65].

Un diagrama de actividades contiene: Estados de actividad, Estados de acción, Transiciones y Objetos. Gráficamente se representa con un conjunto de arcos y nodos. Desde un punto de vista conceptual, el diagrama de actividades muestra cómo fluye el control de unas clases a otras con la finalidad de culminar con un flujo de control total que se corresponde con la consecución de un proceso más complejo. Por este motivo, en un diagrama de actividades aparecerán acciones y actividades correspondientes a distintas clases. Colaborando todas ellas para conseguir un mismo fin. [66].

## 2. BPMN

Business Process Model and Notation (BPMN) es una notación gráfica que describe la lógica de los pasos de un proceso de Negocio. Esta notación ha sido especialmente diseñada para coordinar la secuencia de los procesos y los mensajes que fluyen entre los participantes de las diferentes actividades. BPMN proporciona un lenguaje común para que las partes involucradas puedan comunicar los procesos de forma clara, completa y eficiente. De esta forma BPMN define la notación y semántica de un Diagrama de Procesos de Negocio [67].

BPMN permite a las organizaciones visualizar sus procedimientos internos de negocio de forma gráfica y proporciona la notación estándar para la comunicación de procesos. Además, presenta un sólido enfoque para modelar los procesos de negocio de una organización. Como lenguaje de modelado, es adoptado como el estándar de la industria informática. Para BPMN ese contexto incluye no sólo a analistas o recursos involucrados en IT, sino también sectores gerenciales y administrativos a lo largo de toda la organización [68].

## 3. Lenguaje seleccionado

Para la realización del modelo de proceso de seguridad, se selecciona la notación BPMN. Esta elección se basa en que BPMN es capaz de especificar un proceso en un

diagrama en el que es fácil de leer tanto para los usuarios técnicos como para los usuarios de negocios. Es intuitivo y permite la representación de los detalles complejos del proceso. Sirve como un lenguaje estándar, lo que resuelve el problema defino a la falta de comunicación entre el modelado de procesos y su ejecución.

Cuando los técnicos, los empleados y los gerentes internalizan todos los símbolos y la información, el diagrama se torna fácil de leer y modificar. Los beneficios que aporta son muchos: procesos estandarizados, una comunicación clara y la certeza de la ejecución son sólo algunos de ellos.

## 4. Semántica de BPMN

Para realizar la construcción de un diagrama BPMN es importante conocer su nomenclatura y semántica específica. Los componentes principales se denominan: actividades, eventos, gateways, flujos, datos y swimlanes. Además, se considera el manejo de excepciones del proceso en su flujo esperado o tradicional. Se detallan a continuación, los componentes de BPMN [69].

### Actividades

Representan el trabajo a ser realizado en un proceso. Pueden ser atómicas o compuestas. Existen los siguientes tipos de Actividades: Tarea, Subproceso, Actividad.

#### Tareas

Es una actividad atómica dentro de un proceso donde generalmente un usuario y/o aplicación son utilizados para ejecutarla. En la Tabla 14 se detallan los tipos de tareas con su representación gráfica.

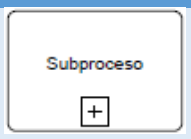
| Tipos de tareas | Diagrama |
|---|---|

| | |
|---|---|
| Servicio: Representa un servicio automatizado provisto por una aplicación. |  |
| Envío: Representa el envío de un mensaje a un participante externo. Cuando el mensaje fue enviado, la tarea finaliza. |  |
| Recepción: Representa la espera del arribo de un mensaje desde un participante externo al proceso. Cuando se recibe el mensaje, la tarea es finalizada. |  |
| Usuario: Tarea de Workflow donde una persona ejecuta la tarea con la asistencia de una aplicación de software y dicha tarea es planificada a través del manejador de lista de trabajos de un BPMS. |  |
| Manual: Tarea que es ejecutada sin la asistencia de una aplicación o BPMS. |  |
| Script: un script ejecutado por una máquina de proceso de un BPMS. El script se define en el lenguaje de script provisto por el BPMS. |  |

**Tabla 14.** Descripción de tipos de tareas.

### Subprocesos

Es una actividad compuesta dentro de un proceso. Presenta tres tipos de subprocesos: embebido, reusable y de evento, transacción. En la Tabla 15 se detallan los tipos de subprocesos con su representación gráfica.

| Tipos de subprocesos | Diagrama |
|---|---|
| Subproceso Embebido: Es un subproceso definido dentro de un proceso pero no puede ser reusado en el contexto de actividades de otro proceso. Usado para definir un alcance dentro de un proceso, para visibilidad, |  |

| | |
|---|---|
| para manejo de transacciones, excepciones, eventos o compensaciones. Puede ser visualizado en forma colapsada o expandida. | |
| Subproceso Reusable: Representa la invocación, en un proceso, a otro proceso predefinido. La invocación resulta en la transferencia de control al proceso llamado. |  |
| Subproceso de Evento: Un subproceso que puede ser iniciado como consecuencia de la ocurrencia de un evento de inicio asociado al mismo. No es parte del flujo de secuencia normal del proceso padre (no tiene flujos de secuencia de entrada y salida). Puede o no ocurrir mientras el proceso padre está en ejecución, pero es posible que ocurra varias veces. Tiene un evento de inicio con un trigger. |  |

**Tabla 15.** Descripción de tipos de subprocesos.

### Marcadores de Tarea y de Subprocesos

Loop: Representa la ejecución repetida de una tarea en forma secuencial. 

## Eventos

Un evento es algo que sucede durante el curso de un proceso de negocio, que afectan el flujo del proceso y generalmente tienen una causa (trigger) o un impacto (resultado). Existen tres tipos de eventos: Inicio, Intermedio y Fin. En la Tabla 16 se detallan los tipos de eventos con su representación gráfica.

| Tipos de eventos | Diagrama |
|---|---|
| Inicio: Indica dónde comienza el flujo de secuencia del proceso. No debe tener ningún flujo de secuencia de entrada. |  |

| | |
|---|---|
| Intermedio: Indican dónde alguna cosa puede ocurrir entre el inicio y el fin de un proceso. |  |
| Fin: Indica dónde finaliza un flujo de secuencia del proceso. No debe tener ningún flujo de secuencia de salida. Un proceso puede tener múltiples eventos de fin. |  |

**Tabla 16.** Descripción de tipos de eventos.

### Gateways

Representan la fusión (división y unión) de flujos. Permiten representar selecciones, paralelismo, fusiones y uniones de caminos. Definen los tipos de comportamiento del flujo de secuencia de un proceso. Dividen y unen los flujos de secuencia. En la Tabla 17 se detallan los tipos de gateways con su representación gráfica.

| Tipos de gateways | Diagrama |
|---|---|
| Exclusive Gateway (XOR): Un punto en un proceso donde el flujo de secuencia puede tomar dos o más caminos alternativos (mutuamente excluyentes). Para cada camino alternativo existe una expresión Condicional. Cuando la evaluación de la expresión de un camino alternativo retorna True, el flujo de secuencia correspondiente es seleccionado. Sólo uno de los caminos será seleccionado, si ningún camino es seleccionado, el camino por defecto será seleccionado (si está definido). |  |
| Event-Based Gateway: Un punto en el proceso donde la selección de los caminos alternativos está basada en la ocurrencia de eventos. El destino de los caminos alternativos es una tarea de recepción o bien un evento intermedio. Puede ser utilizado para comenzar un proceso. |  |

| | |
|---|---|
| Inclusive Gateway (OR): Un punto en un proceso donde el flujo de secuencia puede tomar uno o más caminos alternativos. Es utilizado para crear caminos alternativos como así también paralelos, ya que más de un camino alternativo puede ser Seleccionado. Los caminos alternativos están basados en expresiones lógicas definidas en cada flujo de secuencia de salida, donde cada camino es independiente. |  |
| Parallel Gateway (AND): Usado para crear y sincronizar flujos paralelos, aunque no son necesarios para crear flujos paralelos, pueden ser usados para claridad. |  |

**Tabla 17.** Descripción de tipos de gateways.

### Flujos

Definen la manera de conectar objetos de flujo y artefactos. En la Tabla 18 se detallan los tipos de flujos con su representación gráfica.

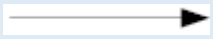
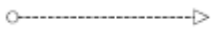
| Tipos de flujos | Diagrama |
|---|---|
| Flujo de Secuencia: Usado para representar el orden de ejecución de las actividades en un proceso. El origen y el destino del flujo de secuencia deben ser uno de los siguientes objetos de flujo: Eventos, Actividades y Gateways. No puede cruzar los límites de un pool (organización). |  |
| Flujo de Mensaje: Usado para representar el flujo de mensajes entre dos participantes que están preparados para enviar y recibir mensajes. |  |
| Asociación: Usada para asociar artefactos con objetos de flujo. |  |
| Asociación de Datos: Usada para asociar datos con objetos de flujo. |  |

**Tabla 18.** Descripción de tipos de flujos.

### Datos

Representan los datos o información consumidos o producidos por las actividades. En la Tabla 19 se detallan los tipos de datos con su representación gráfica.

| Tipos de datos | Diagrama |
|---|---|
| Objetos de Datos: Información que las actividades requieren para ser ejecutadas y/o que producen. Pueden representar un objeto particular o una colección. |  |
| Entradas de Datos: Información requerida para ejecutar un proceso. |  |
| Salidas de Dato: Información producida por un proceso. |  |

**Tabla 19.** Descripción de tipos de datos.

### Swimlanes

Permiten la agrupación de elementos de modelado. En la Tabla 20 se detallan los tipos de swimlanes con su representación gráfica.

| Tipos de swimlanes | Diagrama |
|---|---|
| Pool: Representa un participante (organización) en un proceso. Actúa como un contenedor gráfico para agrupar un conjunto de actividades de un Pool (organización), generalmente en el contexto de escenarios B2B. En otros términos, representa un proceso de una organización. |  |

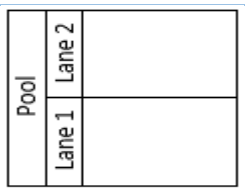
| | |
|---|---|
| Lanes (partición de pool): Una Lanes una sub-partición dentro de un pool. Generalmente usada para categorizar y organizar actividades realizadas por roles o unidades organizacionales. Pueden representar cualquier característica deseada. |  |

**Tabla 20.** Descripción de tipos de swimlanes.

### Excepciones

BPMN no provee un elemento explícito para manejar excepciones, pero sí provee un conjunto de técnicas, que pueden ser representadas mediante:

- Evento de Terminación: Representa cuando se aborta un proceso.
- Eventos Intermedios: Manejo de excepciones con eventos intermedios asociados (boundary events) a una actividad (tarea o proceso). Estos eventos pueden representar:
    - La interrupción de la actividad al ocurrir el trigger del evento: Todo el trabajo que se esté realizando en la actividad será interrumpido y el flujo continuará desde el flujo de salida del evento.
    - La no interrupción de las actividades al ocurrir el trigger del evento: el trabajo que se esté realizando en la actividad NO será interrumpido y el flujo continuará desde el flujo de salida del evento.
- Eventos de Tiempo: Timeouts o Deadlines.
- Subproceso de eventos: Todo el trabajo que se esté realizando en el subproceso será interrumpido y el flujo continuará desde el evento.