INVESTIGACIÓN

Gestión de riesgos técnicos en nubes privadas con soporte a la categoría de servicio IaaS

Management of technical risks in private clouds with support for the IaaS service category

Ing. Anet Fernández Bezanilla[1*], MSc. Lilia R. García Perellada[2], Dr.Sc. Alain A. Garófalo Hernández[3]

Recibido: 03/2018 | Aceptado: 05/2018

PALABRAS CLAVE
Gestión de riesgos
Computación en la nube
Nube privada
Virtualización

RESUMEN

La gestión de riesgos en las nubes privadas adquiere relevancia debido a que, en este tipo de escenario, las amenazas a los centros de datos tradicionales coexisten junto a las que provocan el empleo de los recursos compartidos y otras características de la computación en la nube y la virtualización. En este artículo se presentan los principales riesgos técnicos asociados a este tipo de despliegue y se describen los dos estándares recomendados para la gestión de riesgos. Fueron empleados métodos teóricos de investigación como el análisis histórico-lógico y el dialéctico en el estudio crítico de la bibliografía relacionada con la temática investigada y en la elaboración de la propuesta.

Finalmente, se propone un ciclo de tareas para llevar a cabo el proceso de gestión de riesgos de manera simplificada.

KEYWORDS
Risk management
Cloud computing
Private cloud
Virtualization

ABSTRACT

Risk management in private clouds acquires relevance because, in this type of scenario, the threats of traditional data centers coexist alongside those that cause the use of shared resources and other features of cloud computing and virtualization This paper presents the main technical risks associated with this type of deployment and describes the two recommended standards for risk management. The theoretical methods of investigation, historical-logical analysis and the dialectic were used in the critical study of the bibliography related to the subject under investigation and in the elaboration of the proposal.

Finally, a task cycle is proposed to carry out the risk management process in a simplified manner.

Introducción

La seguridad de la Computación en la Nube (CN) continua siendo uno de los principales requerimientos para lograr la consolidación de este paradigma, como una solución factible y robusta que

1* Empresa Tecnologías de la Información, BioCubaFarma. La Habana, Cuba. anet.fdez@oc.biocubafarma.cu
2 Universidad Tecnológica de La Habana "José Antonio Echeverría". La Habana, Cuba. lilianrosa@tele.cujae.edu.cu
3 Universidad Tecnológica de La Habana "José Antonio Echeverría". La Habana, Cuba. aagarofal@gmail.com

se pueda aplicar en múltiples entornos (Katsikas, 2017; Pattakou y Kalloniatis, 2017). Si bien es cierto que las Nubes Privadas (NP) ofrecen ventajas con respecto a las nubes públicas en lo referente a la gestión de la seguridad, ya que el propietario de la nube tiene el control sobre la infraestructura física y virtual, en ellas coexisten los riesgos de los Centros de Datos (CD) tradicionales, junto a los que se derivan de las características de la virtualización y la CN, tales como el autoservicio bajo demanda, la multitenencia, la rápida escalabilidad y la elasticidad (ENISA, 2017; Felsch y Heiderich, 2015; UIT-T, 2015).

Con respecto al marco regulatorio vigente en Cuba, la Resolución No. 127/2007 del Ministerio de Comunicaciones, establece que cada entidad que haga uso de las tecnologías de la información para el desempeño de su actividad está en la obligación de diseñar, implantar y mantener actualizado un sistema de Seguridad Informática con el objetivo de garantizar la continuidad de los procesos y minimizar los riesgos sobre los sistemas informáticos. Aunque esta resolución carece de actualización y deja muchas lagunas en relación a la gestión de la seguridad, y en especial a la gestión de riesgos, al menos obliga a las entidades a formular una estrategia a seguir ante cualquier incidente o violación de la seguridad, siendo consecuente con sus objetivos básicos y tomando en consideración los riesgos que la entidad enfrenta, en términos de su probabilidad e impacto (Ministerio de Comunicaciones de Cuba, 2007).

La gestión de riesgos es un proceso esencial dentro de la gestión de la seguridad de cualquier organización, la cual tiene por objetivo minimizar las pérdidas y el impacto negativo que puedan provocar esos riesgos. En el caso de las NP, la gestión de riesgos es un factor imprescindible para la detección de las amenazas y vulnerabilidades que puedan ser explotadas, así como para desarrollar una correcta selección y configuración de los controles de seguridad, y definir las prioridades para su implementación en función de los objetivos del negocio. La presente investigación se aborda los principales riesgos técnicos asociados a una NP con soporte a la categoría Infraestructura como *Servicio Infrastructure as a Service* (IaaS), y se analizan los estándares de gestión de riesgos recomendados para estos entornos. Como resultado de la investigación se propone un grupo de tareas específicas para llevar a cabo una gestión de riesgos en este tipo de despliegue.

Materiales y métodos

Para la realización de esta investigación fueron empleados los métodos teóricos de investigación análisis histórico-lógico y el dialéctico en el estudio crítico de la bibliografía relacionada con la temática investigada y en la elaboración de la propuesta.

Resultados y discusión

Los riesgos de seguridad que pueden afectar a una NP con soporte por lo general guardan relación con el contexto, entiéndase diseño físico y lógico de la nube, categoría de servicio que se ofrece y las políticas que se establezcan propias de la organización o derivadas de regulaciones o leyes. El compendio de riesgos técnicos asociados a las NP con soporte a la categoría IaaS que se presenta en la figura 1, fue conformado a partir de un análisis crítico de diferentes fuentes, (Aldossary y Allen, 2016; Bali, 2015; Bazm y Lacoste, 2017; Farahmandian y Hoang, 2016; Gholami, 2016; Hussain y Fatima, 2017; Iqbal y Kiah, 2016; Islam y Manivannan, 2016; Kesavaraj y Anitha, 2016; Krishna, 2015; Kumar, 2016; Laderman y Cox, 2016; Majhi y Dhal, 2016; Rao y Selvamani, 2015; Saini y Saini, 2014; Sushmitha y Reddy, 2015; Vurukonda y Rao, 2016), así como documentos provenientes de organizaciones internacionales como la Alianza para la Seguridad en la Nube (CSA) (Cloud Security Alliance, 2017) y la Unión Internacional de Telecomunicaciones (UIT-T) (UIT-T, 2015).

A partir del análisis, se comprobó que la violación y pérdida de datos es una de las amenazas que generan mayor preocupación, la cual puede ser el objetivo principal de un ataque o simplemente el resultado de errores humanos, vulnerabilidades de los sistemas o prácticas de seguridad deficientes. Aunque el riesgo asociado a esta amenaza suele ser superior en las nubes públicas, también se considera un incidente de seguridad con un alto impacto en las NP cuando datos sensibles o confidenciales son copiados, modificados, eliminados, robados o divulgados por una persona o entidad no autorizada para hacerlo. Estos datos pueden corresponder a información financiera, Información Personal Identificable (PII), secretos empresariales o gubernamentales, propiedad intelectual, e incluso bases de datos (BD), imágenes de máquinas virtuales (MV), archivos de disco virtual, archivos de configu-

ISSN: 1813-5056 Vol. 14, No. 1 , enero-julio, pp. 30 - 40, 2018 tono

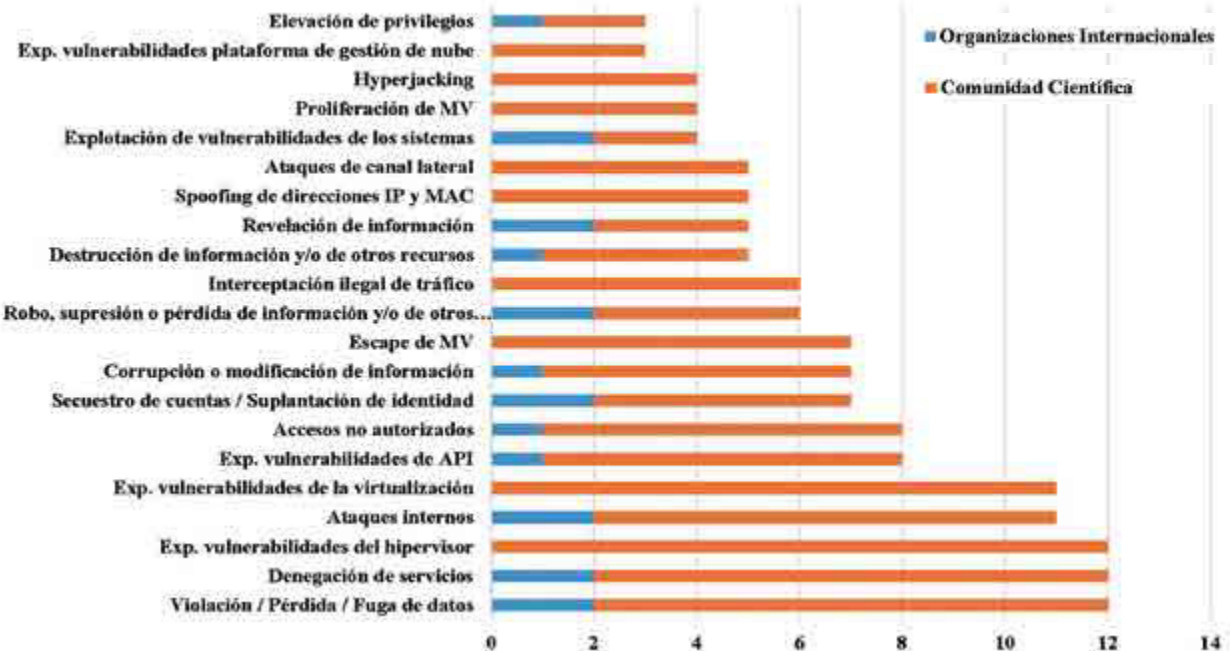

Figura 1. Principales riesgos técnicos en NP con soporte a la categoría IaaS.

ración y datos operacionales (Cloud Security Alliance, 2017; Islam y Manivannan, 2016; Krishna, 2015).

Los riesgos relacionados con la interrupción o denegación de servicios también son especialmente críticos, debido a que pueden afectar tanto a los recursos virtualizados como a la capa física subyacente, y la recuperación y reubicación de los recursos virtuales puede causar la degradación del rendimiento del sistema. Asimismo, los ataques que generan la asignación incontrolada de recursos virtuales de red pueden provocar condiciones de congestión, saturando las capacidades disponibles de la red física (Bays y Oliveira, 2015; ENISA, 2017).

Se evidencia la recurrencia en los riesgos asociados con el hipervisor, el cual constituye una de las principales superficies de ataques, considerándose un elemento de alta criticidad, debido a que cualquier vulnerabilidad que sea explotada en el mismo, puede poner en riesgo la seguridad de la infraestructura asociada. A su vez, las herramientas de gestión de la virtualización y el conjunto de Interfaces de Programación de Aplicaciones (API) de administración remota de los hipervisores, generan nuevos vectores de ataques. Garantizar la seguridad de la capa de virtualización es fundamental debido a que toda la plataforma de nube está sustentada por una infraestructura virtualizada, y por consiguiente, una violación a la seguridad de la misma supone una puerta a posibles ataques a la plataforma de nube, a las capas de servicio y a los datos (ENISA, 2017).

Muchos de esos riesgos son generados por problemas de operación y configuración, siendo los más recurrentes: la gestión inadecuada de los roles de administración de la plataforma de virtualización y gestión de nube, el control ineficiente del ciclo de vida de las MV y los procesos de gestión de cambios y chequeo de integridad; la no centralización, monitoreo y análisis continuo de los eventos para la detección de anomalías y no adoptar las mejores prácticas recomendadas por los proveedores. (ENISA, 2017)

Existe otro grupo de riesgos asociados con errores o debilidades de software que pueden ser explotados de manera malintencionada. Estas amenazas constituyen un riesgo aún mayor, debido a que el atacante puede tomar el control de un gran número de recursos virtuales de manera rápida y simultánea. Entre las vulnerabilidades más frecuentemente explotadas se destacan aquellas que permiten la elevación de privilegios, la inyección y ejecución de código arbitrario, la revelación de información y la denegación de servicios (ENISA, 2017; Laderman y Cox, 2016). La información relativa a las vulnerabilidades de software es registrada por la organización estadounidense MITRE, patrocinada por el Departamento de Seguridad Nacional de los Estados Unidos, y está disponible para su conocimiento pú-

blico en el sitio web: "Common Vulnerabilities and Exposures" (MITRE, 2018) y en la Base de Datos Nacional de Vulnerabilidades del Instituto Nacional de Estándares y Tecnologías (NIST, 2018).

Estándares para la gestión de riesgos

La gestión de riesgos es un proceso cíclico que comprende la identificación de los riesgos, su evaluación, una estrategia para su mitigación, y la selección e implementación de técnicas y procedimientos para su monitoreo continuo (Gartner, 2018; NICCS, 2018). Existen varios estándares y metodologías que ofrecen directrices y principios para la gestión de los riesgos en los sistemas de información, aunque no se han desarrollado normas específicas para los modelos de despliegue ni de servicio de la CN. El estándar 27017:2015 de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), plantea que, tanto los clientes como los proveedores del servicio de nube deben tener información acerca de los procesos de gestión de riesgos, y recomienda el uso de los estándares ISO 31000:2009[1] e ISO/IEC 27005:2011 (International Organization for Standardization, 2015). Por su parte la CSA menciona como una alternativa factible a las normas de la ISO, el Marco de Gestión de Riesgos definido por el NIST, el cual se aborda en varias de sus Publicaciones Especiales (SP), presentándose específicamente una guía para su aplicación en la SP 800-37 rev.1[2]. (Cloud Security Alliance, 2017)

Gestión de riesgos según la ISO

El estándar internacional ISO 27005:2011, actualmente bajo revisión, proporciona una guía para la gestión del riesgo de seguridad de la información en una organización, en apoyo a los requerimientos del sistema de gestión de seguridad definido en el estándar ISO/IEC 27001. El estándar es una adaptación de la norma ISO 31000:2009[3], la cual provee directrices genéricas y un marco de referencia para el diseño, la implementación y el soporte del proceso de gestión de riesgos en cualquier contexto (International Organization for Standardization, 2011).

La ISO define el riesgo como el efecto de la incertidumbre en los objetivos, en lugar de la probabilidad de ocurrencia de un evento con impacto en los objetivos (International Organization for Standardization, 2011). Esto quiere decir que se considera el riesgo como neutral, ya que las consecuencias asociadas con un riesgo pueden ser positivas o negativas, mejorando o limitando el logro de los objetivos definidos en cualquier nivel: estratégico, organizacional y tecnológico. En muchas organizaciones, la gestión de riesgos con consecuencias positivas, referida como oportunidades, se separa de la gestión de riesgos con consecuencias negativas o simplemente no se tiene en cuenta. El proceso de gestión de riesgos, como se muestra en la figura 2, debe ser un proceso constante, integrado en las actividades de gestión de la seguridad y se estructura de la siguiente forma:

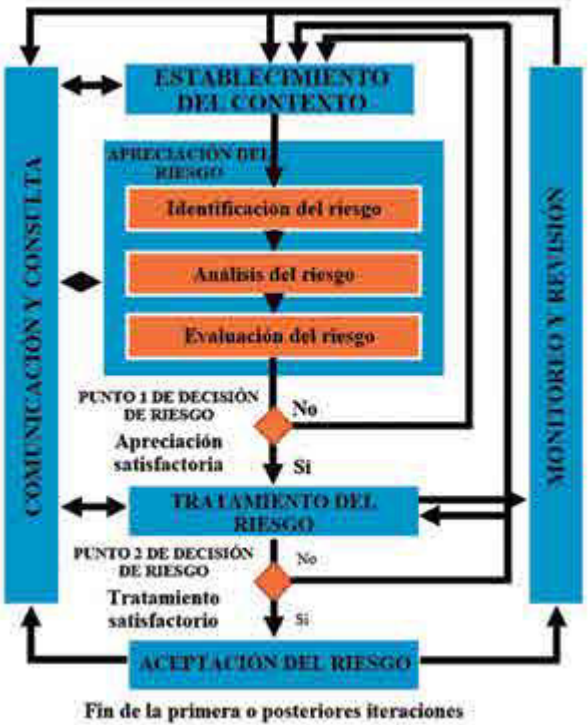

Figura 2. Proceso de gestión de riesgos definido por la ISO/IEC 27005:2011

Establecimiento del contexto externo e interno: Consiste en organizar el proceso de gestión de riesgos, definiendo las responsabilidades, el alcance y el ámbito de aplicación, así como un grupo de criterios básicos necesarios tales como la evaluación, el impacto y la aceptación de los riesgos.

1 La norma ISO 31000 fue actualizada en febrero de 2018.

2 En mayo de 2018 el NIST publicó a modo de borrador la Revisión 2 de esta guía.

3 La ISO 31000:2009 se complementa con un vocabulario formal de definiciones (ISO 73:2009), y con un conjunto de técnicas de evaluación de riesgos (ISO/IEC 31010:2009), este último está bajo actualización.

ISSN: 1813-5056 Vol. 14, No. 1 , enero-julio, pp. 30 - 40, 2018 tono

Apreciación del riesgo: comprende las tareas de identificación, análisis y evaluación de los riesgos. Se determina el valor de los activos de información, se identifican las amenazas y vulnerabilidades existentes o que puedan existir, así como los controles de seguridad y su efecto. Finalmente, se analizan las consecuencias potenciales, se clasifican los riesgos de acuerdo a los criterios definidos en el establecimiento del contexto y se establecen prioridades para ayudar en la toma de decisiones en la etapa de tratamiento.

Tratamiento del riesgo: consiste en seleccionar e implementar controles que permitan alguna de las siguientes opciones: modificar, conservar, evitar o compartir el riesgo. Puesto que los riesgos nunca desaparecerán totalmente, la dirección de la entidad debe asumir un riesgo residual, o sea el nivel restante de riesgo después de su tratamiento.

Comunicación y consulta: facilita los intercambios de información sobre riesgos entre las partes interesadas externas e internas de manera bidireccional. Esta información incluye la existencia, naturaleza, probabilidad, severidad, tratamiento y aceptabilidad de los riesgos. Una comunicación efectiva puede tener un impacto significativo en las decisiones que se tomen respecto al riesgo.

Seguimiento y revisión: Resulta necesario monitorear y revisar de manera constante las amenazas, vulnerabilidades, probabilidad de ocurrencia, y consecuencias de los riesgos con el fin de detectar cambios en el contexto. Esto permitirá identificar de manera oportuna riesgos emergentes y determinar si los controles aplicados son eficaces.

Con relación al análisis de riesgos, resulta oportuno aclarar que este proceso puede ser llevado a cabo con diferentes niveles de detalle, en dependencia de la criticidad de los activos, el grado de las vulnerabilidades conocidas y los incidentes previos que involucran a la organización. La metodología de análisis de riesgos puede ser cualitativa, cuantitativa o una combinación de ambas. En la práctica, los análisis cualitativos son empleados a menudo en un primer momento para obtener una idea aproximada del nivel de riesgo e identificar los más relevantes. Por lo general, en el análisis cualitativo se emplean los atributos calificativos Bajo, Medio y Alto para describir la magnitud del impacto potencial y su probabilidad de ocurrencia. Por su parte, los análisis cuantitativos se realizan generalmente sobre los riesgos más significativos y la escala numérica varía de una propuesta a otra. En ambos casos es común el empleo de Matrices de Riesgos para determinar el nivel de riesgo del activo (International Organization for Standardization, 2011). Existen sistemas como el *Open Source Security Information Management*[4] (OSSIM), que calculan de manera automática, dado un valor de activo dado, el nivel de riesgo a partir de correlacionar la información obtenida por el escáner de vulnerabilidades y las alertas generadas por los Sistemas de Detección de Intrusos (IDS).

Gestión de riesgos según el NIST

El NIST define el riesgo como la probabilidad de ocurrencia de una amenaza potencial y su nivel de impacto en las operaciones, activos y personas de una organización, e incluso de terceros que puedan ser afectados. La gestión de riesgos (Figura 3) se describe como una actividad holística, completamente integrada dentro de la organización, la cual comprende: el proceso de evaluación de riesgos; un marco de gestión, que establece el contexto para la toma de decisiones basadas en el riesgo; la respuesta a estos una vez determinados y

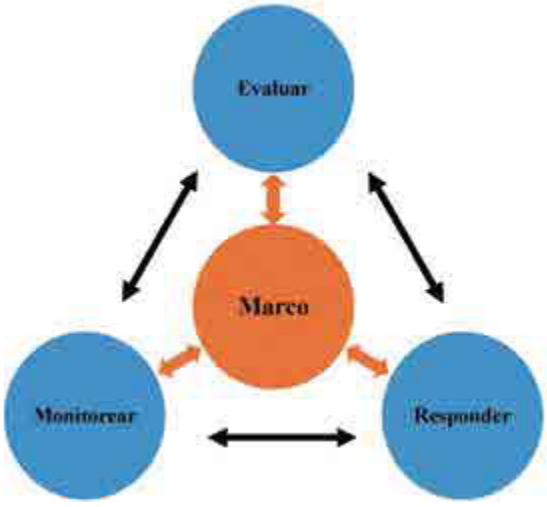

Figura 3. Proceso de gestión de riesgos descrito por el NIST

la monitorización que posibilite una retroalimentación de información para la mejora continua de la gestión de riesgos. (NIST, 2012)

El proceso de evaluación de riesgos (Figura 4) está compuesto por diferentes tareas agrupadas en cuatro etapas:

Preparación: Determinar el propósito y el alcance de la evaluación, identificar suposiciones y limitaciones asociadas con el proceso de evaluación, identificar

4 Sistema de Gestión de Eventos e Información de Seguridad (SIEM) de Software Libre y Código Abierto (SLCA) de Alienvault.

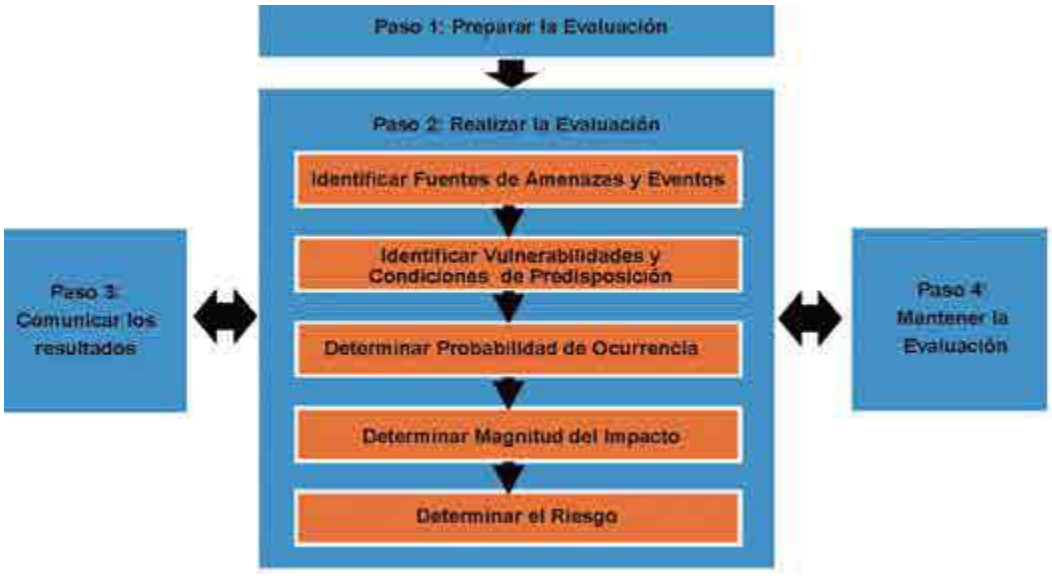

Figura 4. Tareas comprendidas en el proceso de evaluación de riesgos establecido por el NIST

las fuentes de información a ser usadas como entradas para la evaluación e identificar el modelo de riesgos y el enfoque analítico que serán empleados.

Ejecución: Identificar las fuentes de amenazas relevantes a la organización, y los eventos que se pueden generar desde esas fuentes. Identificar las vulnerabilidades que pueden ser explotadas por las fuentes de amenazas mediante eventos específicos y las condiciones que propician que la explotación sea efectiva. Determinar la probabilidad de que las fuentes de amenazas identificadas puedan iniciar un evento de seguridad específico y la probabilidad de que el evento sea exitoso. Determinar el impacto negativo de esos eventos sobre las operaciones, los activos y los individuos de la organización. Determinar los riesgos de seguridad de la información como combinación de la probabilidad de la explotación de vulnerabilidades y su impacto, incluyendo cualquier incertidumbre asociada con la determinación de los riesgos.

Comunicación de los resultados: Comunicar los resultados de la evaluación de riesgos a los decisores y compartir la información obtenida durante la ejecución de la evaluación de riesgos, para contribuir a otras actividades del proceso de gestión de riesgos.

Mantenimiento: Monitorear los factores de riesgo identificados en la evaluación, considerando los cambios asociados a esos factores. Actualizar los componentes de la evaluación de riesgos reflejando las actividades de monitoreo llevadas a cabo por la organización. Esto permite identificar cambios en el impacto de los riesgos en los sistemas de información y en el ambiente en que ellos operan así como determinar la efectividad de la respuesta a los riesgos.

El marco de gestión de riesgos desarrollado por el NIST (Figura 5) puede ser usado en diversos entornos expuestos a vulnerabilidades y amenazas crecientes de diferentes niveles de complejidad. Este marco promueve el concepto de gestión de riesgos "casi en tiempo real" y fomenta el uso de la automatización para proveer a directivos y decisores, de la información necesaria para tomar decisiones rentables basadas en el riesgo, con respecto a los sistemas de información de la organización que soportan las misiones y funciones principales del negocio.

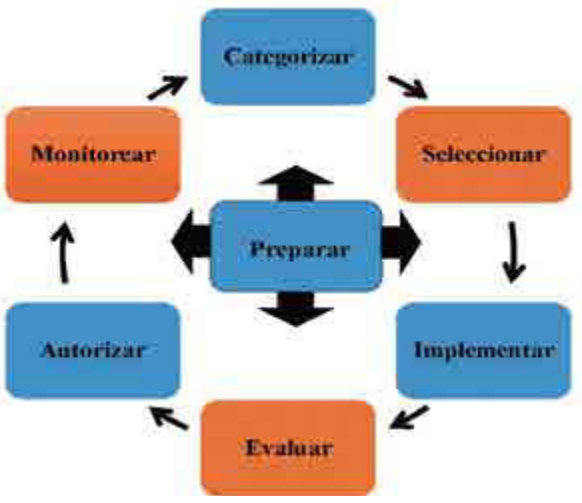

Figura 5. Marco de gestión de riesgos elaborado por el NIST (Fuente: NIST, 2018b).

Como se observa, el marco está conformado por los siguientes procesos:

- Preparación inicial para establecer el contexto donde se ejecutará el marco de gestión de riesgos, desde una perspectiva organizacional y a nivel de sistema. Comprende, entre otras tareas: la definición de la estrategia de gestión de riesgos para la organización, la asignación de roles para ejecutar la gestión de riesgos, la evaluación de los riesgos, la identificación de activos y tipos de información, la priorización de los sistemas organizacionales con el mismo nivel de impacto y la definición de requerimientos de seguridad y privacidad.

- Categorización de los sistemas de información y la información procesada, almacenada y transmitida por los sistemas, basado en un análisis de impacto.[5]

- Selección de un grupo inicial de controles de seguridad a partir de la categorización anterior, teniendo en cuenta la evaluación de riesgos y las condiciones locales.[6]

- Implementación de los controles de seguridad, describiendo cómo esos controles son empleados dentro de los sistemas de información y su ambiente de operación.

- Evaluación de los controles de seguridad, para determinar en qué medida están correctamente implementados, operando en un estado deseado, produciendo el resultado esperado y cumpliendo con los requerimientos de seguridad del sistema.

- Autorización de la operación de los sistemas de información, basado en un nivel de riesgo aceptable para las operaciones, los activos y los individuos de la organización.

- Monitorización de los controles de seguridad, incluyendo la evaluación de su eficacia, la documentación de cambios en el sistema o en su ambiente de operación, el respectivo análisis de su impacto en la seguridad y la generación de reportes sobre el estado de seguridad del sistema a los especialistas.

Propuesta de gestión de riesgos técnicos para una NP con soporte a la categoría IaaS.

En el caso de una NP con soporte a la categoría IaaS, algunas de las metodologías de gestión de riesgos empleadas en los CD tradicionales como Octave, Magerit y Mehari pudieran ser aplicadas. Especialmente hay que considerar que la capa de gestión de la nube y de la infraestructura de virtualización implican que determinados riesgos tengan un impacto mucho mayor, como por ejemplo la explotación de vulnerabilidades en estas plataformas y la modificación de permisos y configuraciones. El proceso de gestión de riesgos que se propone (Figura 6) debe ser cíclico y en constante perfeccionamiento, siendo un requisito indispensable que cada organización defina un marco temporal para la ejecución de las siguientes tareas:

- Inventario automatizado de activos (físicos y virtuales). Estimar un valor para cada activo (asignar un valor máximo a la infraestructura de virtualización y gestión de la nube).

- Listado de vulnerabilidades obtenido de herramientas de escaneo automatizado (ej. OpenVAS). Puede resultar útil la información resultante de las pruebas de penetración realizadas en las auditorías.

- Identificar las Amenazas. Comprende la detección de incidentes, el análisis de eventos y la correlación de información (automática o manual). Por lo general, se despliegan IDS de red (ej. Suricata) y de servicios (ej. OSSEC), SIEM (ej. OSSIM), Plataformas de Antivirus y de Inteligencia de Amenazas, en todos los casos con soporte para virtualización.

- La efectividad de los controles de seguridad implementados, ya sean preventivos, de detección o de recuperación. Entre los controles más significativos se encuentran: gestión de actualizaciones y parches (incluyendo MV inactivas); fortalecimiento del hipervisor y las MV; gestión de configuraciones y control de cambios; protección criptográfica, protección antivirus, antispam y web; protección perimetral (zonas de diferentes niveles de confianza mediante cortafuegos virtualizados); control de accesos y gestión de identi-

5 En el 2004 fue publicado en Estados Unidos el estándar FIPS 199 para la Categorización de Seguridad de la Información Federal y los Sistemas de Información. El análisis de impacto se refiere a determinar en qué medida un cambio en el sistema de información ha afectado o puede afectar la postura de seguridad del sistema, calificado como "Bajo", "Moderado" o "Alto".

6 Los controles definidos por el NIST para la privacidad y la seguridad de los Sistemas de Información Federales y Organizaciones de Estados Unidos se describen en la SP 800-53 Rev. 4. Estos controles han sido actualizados en varias ocasiones, teniendo en cuenta la sofisticación creciente de los ataques en el ciberespacio. Actualmente el NIST trabaja en la elaboración de la Revisión 5, la cual ya está disponible a modo de borrador.

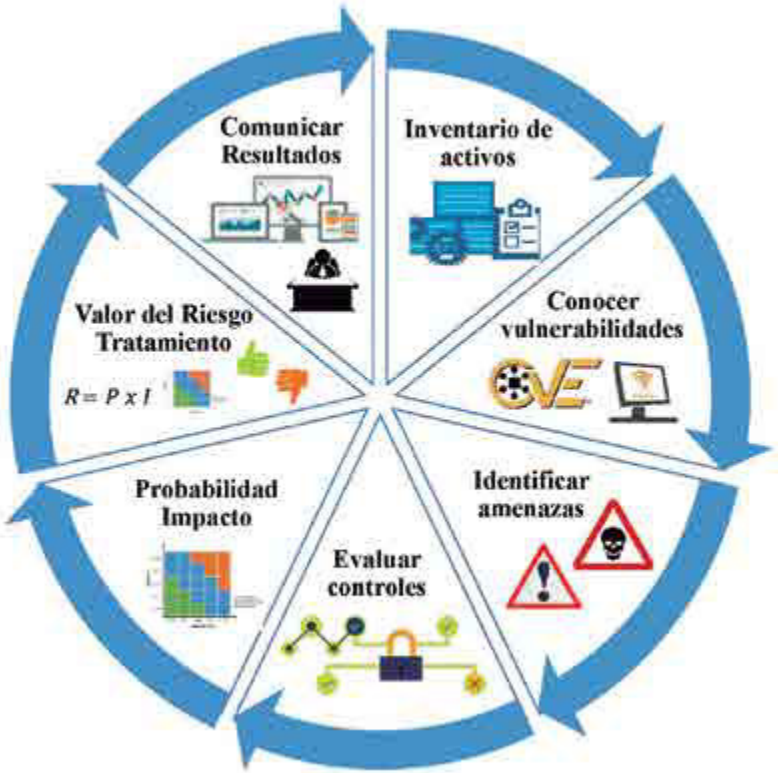

Figura 6. Proceso de gestión de riesgos técnicos propuesto para una NP con soporte para IaaS.

dades; monitoreo y gestión centralizada de los registros de auditoría y gestión de salvas y restauración.

- La probabilidad de ocurrencia y el impacto. Puede medirse cualitativamente en Muy Bajo, Bajo, Medio, Alto, Muy Alto o usando una escala numérica. En el caso de la probabilidad resulta difícil realizar una estimación sin tener datos de incidentes previos similares en la organización.

- La probabilidad del valor del riesgo (Probabilidad por Impacto), permite establecer las prioridades y definir su tratamiento (fundamentalmente modificarlo o evitarlo, aunque por análisis de costo beneficio puede resultar factible conservarlo). La decisión del tratamiento del riesgo debe ser aprobada por la dirección. Puede conllevar a implementar nuevos controles o realizar cambios en las configuraciones existentes.

- Elaborar reporte, registrar y comunicar resultados a la dirección y demás partes interesadas.

El marco temporal que se establezca dependerá de la cantidad de activos de la entidad, la frecuencia de publicaciones de vulnerabilidades que puedan afectar esos activos y la periodicidad con la que son publicadas actualizaciones de software, parches de seguridad y firmas para detectar y mitigar esas amenazas. Para organizaciones pequeñas el proceso de gestión de riesgos puede realizarse de manera mensual, sin embargo, para aquellas con un número considerable de activos puede ser conveniente realizarlo dos o tres veces al año, priorizando la ejecución de las tareas definidas en los puntos dos, tres y cuatro. Es importante destacar que el proceso de gestión de riesgos debe estar planificado, documentado sus procedimientos y aprobado por la dirección de cada entidad como parte de las políticas de gestión de seguridad.

Conclusiones

La gestión de riesgos debe estar concebida en las tareas estratégicas, de gestión y operacionales de una organización mediante sus funciones y procesos, adaptándose a las necesidades del negocio, sus objetivos particulares, el contexto y prácticas específicas empleadas. Aunque solamente fueron analizados los riesgos técnicos, en los entornos de la CN deberán tenerse en cuenta además otros factores de riesgo importantes como son los medioambientales, los asociados con políticas, con los proveedores y por supuesto con los recursos humanos.

ISSN: 1813-5056 Vol. 14, No. 1 , enero-julio, pp. 30 - 40, 2018 tono

La selección de qué estándar, metodología y sistemas para la gestión de riesgos a utilizar es una decisión de cada organización, pudiendo ser empleados para ese proceso otros documentos con enfoques diferentes a los analizados. Sin embargo, se considera que deben gestionarse aquellos riesgos y combinaciones de estos con posibilidad de materializarse en el contexto y provocar un efecto negativo en la organización, apoyándose en el compendio de riesgos técnicos presentado. Esta propuesta presentada pretende simplificar el proceso de gestión de riesgos, que por lo general resulta complejo, aun cuando la organización sea una pequeña empresa.

Referencia

Katsikas, S. (2017). SEPRICC: Security and Privacy in Cloud Computing. Presentado en Cloud Comuting 2017: The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, Grecia. Disponible en https://www.iaria.org/conferences2017/filesCLOUDCOMPUTING17/SEPRICC_CLOUDCOMPUTING17.pdf

Pattakou, A. y Kalloniatis, C. (2017). Security and Privacy Requirements Engineering Methods for Traditional and Cloud-Based Systems: A Review. Presentado en Cloud Computing 2017: The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, Grecia. Disponible en https://www.thinkmind.org/download.php?articleid=cloud_computing_2017_8_10_28013

ENISA. (2017). Security aspects of virtualization. Disponible en https://www.enisa.europa.eu/publications/security-aspects-of-virtualization/at_download/fullReport

Felsch, D. y Heiderich, M. (2015). How Private is Your Private Cloud? Security Analysis of Cloud Control Interfaces (pp. 5-16). Presentado en ACM Cloud Computing Security Workshop. Disponible en http://dl.acm.org/citation.cfm?doid=2808425.2808432

UIT-T. (2015). Recomendación X.1601. Marco de seguridad para la computación en la nube. Disponible en https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12613

Ministerio de Comunicaciones de Cuba. (2007). «Resolución No. 127/2007. Reglamento de Seguridad Informática». Disponible en http://www.mincowww.mincom.gob.cu/sites/default/files/marcoregulatorio/1346872659054_R 127-07 Reglamento de Seguridad Informatica.pdf

Aldossary, S. y Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: issues and current solutions. International Journal of Advanced Computer Science and Applications, 7(4). Disponible en https://thesai.org/Downloads/Volume7No4/Paper_64-Data_Security_Privacy_Availability_and_Integrity.pdf

Bali, P. (2015). Cloud Computing: Security Issues In Infrastructure-As-A-Service Model. International Journal of in Multidisciplinary and Academic Research, 4(5). Disponible en http://ssijmar.in/vol4no5/vol4%20no5.5.pdf

Bazm, M.-M. y Lacoste, M. (2017). Side Channels in the Cloud: Isolation Challenges, Attacks, and Countermeasures. Disponible en https://hal.inria.fr/hal-01591808/document

Farahmandian, S. y Hoang, D. B. (2016). Security for Software-Defined (Cloud, SDN and NFV) Infrastructures - Issues and Challenges (pp. 13-24). Presentado en Eight International Conference on Network and Communications Security. Disponible en https://doi.org/10.5121/csit.2016.61502

Gholami, A. (2016). Security and Privacy of Sensitive Data in Cloud Computing (Tesis de Doctorado). KTH Royal Institute of Technology, Department of Computational Science and Technology. Estocolmo, Suecia. Disponible en http://www.diva-portal.org/smash/record.jsf?pid=diva2:925669

Hussain, S. A. y Fatima, M. (2017). Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics, 13(1), 57-65. Disponible en https://doi.org/10.1016/j.aci.2016.03.001

Iqbal, S. y Kiah, M. L. M. (2016). Service delivery models of cloud computing: security issues and open challenges: Cloud computing security. Security and Communication Networks, 9(17). Disponible en https://doi.org/10.1002/sec.1585

Islam, T. y Manivannan, D. (2016). A Classification and Characterization of Security Threats in Cloud Computing. International Journal of Next-Generation Computing, 7(1). Disponible en https://www.researchgate.net/profile/Tariqul_Islam16/publication/308172311_A_Classification_and_Characterization_of_Security_Threats_in_Cloud_Computing/links/57dc38cf08aeea195935c51f/A-Classification-and-Characterization-of-Security-Threats-in-Cloud-Computing.pdf

Kesavaraj, G. y Anitha, K. (2016). Addressing Cloud Computing Security Issues. International Journal of Innovative Research in Computer and Communication Engineering, 4(6). Disponible en https://www.ijircce.com/upload/2016/june/228_ADDRESSING.pdf

Krishna, V. (2015). Security Issues and Countermeasures in Cloud Computing Environment. International Journal of Engineering Science and Innovative Technology, 4(5), 5.

Kumar, P. (2016). Cloud Computing: Threats, Attacks and Solutions. International Journal of Emerging Technologies in Engineering Research, 4(8). Disponible en http://www.ijeter.everscience.org/Manuscripts%5CVolume-4%5CIssue-8%5CVol-4-issue-8-M-06.pdf

Laderman, E. y Cox, K. (2016). Resiliency Mitigations in Virtualized and Cloud Environments (MITRE Technical Report). Disponible en https://www.mitre.org/sites/default/files/publications/pr-16-3043-virtual-machine-attacks-and-cyber-resiliency.pdf

Majhi, S. K. y Dhal, S. K. (2016). A Study on Security Vulnerability on Cloud Platforms. Procedia Computer Science, 78, 55-60. Disponible en https://doi.org/10.1016/j.procs.2016.02.010

Rao, R. V. y Selvamani, K. (2015). Data Security Challenges and Its Solutions in Cloud Computing. Procedia Computer Science, 48, 204-209. Disponible en https://doi.org/10.1016/j.procs.2015.04.171

Saini, H. y Saini, A. (2014). Security Mechanisms at different Levels in Cloud Infrastructure. International Journal of Computer Applications, 108(2). Disponible en http://search.proquest.com/openview/65a400aace0f24bcf33db2b81e184914/1?pq-origsite=gscholar&cbl=136216

Sushmitha, Y. y Reddy, V. K. (2015). A survey on cloud computing security issues. International Journal of Computer Science and Innovation, 2015(2). Disponible en https://www.researchgate.net/publication/299569834_A_Survey_On_Cloud_Computing_Security_Issues

Vurukonda, N. y Rao, B. T. (2016). A Study on Data Storage Security Issues in Cloud Computing. Presentado en 2nd International Conference on Intelligent Computing, Communication & Convergence. Disponible en https://doi.org/10.1016/j.procs.2016.07.335

Cloud Security Alliance. (2017b). The Treacherous 12 - Top Threats to Cloud Computing + Industry Insights. Disponible en https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf

Bays, L. R. y Oliveira, R. R. (2015). Virtual network security: threats, countermeasures, and challenges. Journal of Internet Services and Applications, 6(1). Disponible en https://doi.org/10.1186/s13174-014-0015-z

MITRE. (2018). CVE - Common Vulnerabilities and Exposures. Accedido 10 de julio de 2018, Disponible en https://cve.mitre.org/

NIST. (2018a). National Vulnerability Database (NVD). Accedido 10 de julio de 2018, Disponible en https://nvd.nist.gov/

Gartner. (2018). IT Glossary: Integrated Risk Management (IRM). Accedido 10 de julio de 2018, Disponible en https://www.gartner.com/it-glossary/integrated-risk-management-irm/

NICCS. (2018). A Glossary of Common Cybersecurity Terminology [Official website of the Department of Homeland Security of USA]. Accedido 10 de julio de 2018, Disponible en https://niccs.us-cert.gov/glossary

International Organization for Standardization. (2015). ISO/IEC 27017:2015. Code of practice for information security controls based on ISO/IEC 27002 for cloud services. Disponible en https://www.iso.org/standard/43757.html

Cloud Security Alliance. (2017a). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. Disponible en https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf

International Organization for Standardization. (2011). ISO/IEC 27005:2011. Information security risk management. Disponible en https://www.iso.org/standard/56742.html

NIST. (2012). Special Publication 800-30 Rev. 1. Guide for Conducting Risk Assessments. Disponible en http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST. (2018b). Special Publication 800-37 rev. 2 Draft. Risk Management Framework for Information Systems and Organizations. Disponible en https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-draft-ipd.pdf

NIST. (2018c). «Special Publication 800-37 rev. 2 Draft. Risk Management Framework for Information Systems and Organizations». Disponible en https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-draft-ipd.pdf