TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 17. No. 1, enero-abril, 2018, p.56- 72 ISSN 1729-3804

PROPUESTA DE CONTROLES DE SEGURIDAD PARA NUBES PRIVADAS Y CENTROS DE DATOS VIRTUALIZADOS

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

[1]e-mail: mailto:anet@eti.biocubafarma.cu, [2]e-mail: mailto:lilianrosa@tele.cujae.edu.cu,

[3]e-mail: mailto:aagarofal@gmail.com

[1]ETI, Grupo BioCubaFarma, calle 18 #4310 e/ 43 y 47, Miramar, Playa, La Habana, Cuba, [2]Universidad Tecnológica de La Habana José Antonio Echeverría (CUJAE), calle 114 e/ Ciclovía y Rotonda, Marianao, La Habana, Cuba, [3]CUJAE, calle 114 e/ Ciclovía y Rotonda, Marianao, La Habana, Cuba

RESUMEN

Las organizaciones con limitaciones de financiamiento, que tienen desplegados centros de datos virtualizados y nubes privadas, se enfrentan al desafío de seleccionar los controles de seguridad que resulten adecuados para reducir los riesgos a un nivel aceptable, y garantizar el cumplimiento de las regulaciones y estándares. En este trabajo se realiza un análisis comparativo de los controles establecidos por las principales organizaciones internacionales de estandarización, incluyendo las regulaciones vigentes en Cuba y Estados Unidos. Tomando como base dicho análisis se propone el mínimo conjunto de controles de seguridad que deben ser implementados, teniendo en cuenta las características y amenazas propias de este modelo de despliegue. Finalmente se presentan algunas soluciones de software libre y código abierto que pueden ser útiles para la implementación de algunos de los controles de seguridad propuestos.

PALABRAS CLAVE: Computación en la Nube, Controles de Seguridad, Nubes Privadas, Virtualización.

SECURITY CONTROLS FOR PRIVATE CLOUDS AND VIRTUALIZED DATA CENTERS

ABSTRACT

Organizations with funding limitations, which have deployed virtualized data centers and private clouds, face the challenge to select appropriate security controls to reduce risks on acceptable levels, then to ensure compliance based on regulations and standards. In this paper, a comparative analysis regarding controls established by the main international organizations of standardization is made, including regulations in Cuba and the United States. Based on these analysis, we propose the minimum set of security controls that must be implemented, given the characteristics and threats inherent to this

deployment model. Finally, some free software and open source solutions are presented that may be useful to implement some of the proposed security controls.

KEYWORDS: Cloud Computing, Security Controls, Private Clouds, Virtualization.

INTRODUCCIÓN

Los controles de seguridad consisten en cualquier método administrativo, gerencial, técnico o legal que se use para modificar un riesgo. El riesgo se puede definir como la probabilidad de ocurrencia de una amenaza potencial y su impacto negativo en las operaciones, activos y personas de una organización, e incluso de terceros que puedan ser afectados. El objetivo fundamental de los controles es satisfacer los requerimientos de seguridad que establezca cada organización y habilitar capacidades para identificar, prevenir y mitigar los riesgos asociados con la pérdida de los Requerimientos no Funcionales (RNF) de seguridad1, tales como la confidencialidad, la privacidad, la disponibilidad y el no repudio. Por lo general están compuestos por un conjunto de políticas, procesos, procedimientos, prácticas, dispositivos y soluciones tecnológicas [1,2].

El grado de seguridad provisto por los controles puede variar de una entidad a otra, ya que depende de los objetivos del negocio, los requerimientos derivados de regulaciones o leyes, la categoría de servicio de Computación en la Nube (CN) que se ofrece, el tipo de información que se gestiona, las tecnologías implementadas y por supuesto el presupuesto destinado a la seguridad [3,4]. Muchas entidades no disponen de los recursos financieros para acceder a soluciones comerciales de seguridad, cuyos costos son elevados. Estas organizaciones se enfrentan al reto de seleccionar e implementar controles de seguridad que permitan cumplir los requerimientos que imponen las regulaciones existentes y enfrentar el panorama de amenazas actual. En el caso de las Nubes Privadas (NP), a estas amenazas se añaden los riesgos derivados de las características de la virtualización y la CN tales como la multitenencia, el autoservicio bajo demanda, y la rápida escalabilidad y elasticidad.

En este trabajo se realiza un análisis comparativo de los controles de seguridad establecidos por las principales organizaciones internacionales de estandarización, y las regulaciones nacionales en los casos de Estados Unidos y Cuba. A partir de este análisis se propone el mínimo conjunto de controles de seguridad que deben ser implementados en una NP o Centro de Datos (CD) virtualizado, teniendo en cuenta las características y amenazas propias de este modelo de despliegue. Finalmente se plantean aspectos para la selección de soluciones de Software Libre y Código Abierto (SLCA) que pueden ser útiles para la implementación de uno o varios de los controles de seguridad seleccionados, y se proponen algunas soluciones.

[1] Los RNF son descritos como propiedades o atributos que caracterizan un sistema, y que permiten juzgar su funcionamiento general en lugar de sus comportamientos específicos.

CONTROLES DE SEGURIDAD DEFINIDOS POR LAS PRINCIPALES ORGANIZACIONES INTERNACIONALES Y LAS REGULACIONES NACIONALES (CASOS: ESTADOS UNIDOS y CUBA)

Al analizar la información proveniente de las organizaciones internacionales líderes en los procesos de estandarización, y regulaciones nacionales en los casos específicos de Estados Unidos y de Cuba, resultaron relevantes algunas normas y recomendaciones que abordan los controles de seguridad para los Sistemas de Información (SI) y los ecosistemas de nube, los cuales se muestran en la Tabla 1.

Tabla 1: Documentos analizados que abordan los controles de seguridad para los SI.

Organizaciones	Estándares y Documentos	Controles descritos	Específica para sistemas de nube	Específica para un país	Fecha de publicación	Referencias
Organización Internacional de Normalización (ISO)[2] / Comisión Electrotécnica Internacional (IEC)[3]	ISO/IEC 27017:2015[4]	121 controles organizados en 14 dominios	sí	no	2015	[5]
Instituto Nacional de Estándares y Tecnologías de Estados Unidos (NIST)[5]	SP[6] 800-53 Revisión 5 (Borrador)	276 controles organizados en 20 familias	no	Estados Unidos	2017	[6]
Alianza para la Seguridad en la Nube (CSA)[7]	Matriz de Controles de la Nube (CCM)[8] versión 3.0.1	133 controles organizados en 16 dominios	sí	no	2017	[7]
Centro para la Seguridad de Internet (CIS)[9]	20 controles críticos de CIS versión 7	20 controles generales (171 subcontroles)	no	no	2018	[8]
Ministerio de Comunicaciones	Resolución No. 127	89 artículos	no	Cuba	2007	[9]

[2] *International Organization for Standardization*
[3] *International Electrotechnical Commission*
[4] Este estándar, el cual se corresponde con la Recomendación X.1631 de la Unión Internacional de Telecomunicaciones (UIT-T), es una modificación de la guía de implementación de los controles definidos previamente en la norma ISO/IEC 27002:2013, fundamentalmente los relacionados con el control de accesos, el cumplimiento, y la seguridad de las operaciones y las comunicaciones.
[5] *National Institute of Standards and Technology*
[6] *Special Publication*
[7] *Cloud Security Alliance*
[8] *Cloud Control Matrix*
[9] *Center for Internet Security*

de Cuba (MINCOM)	/2007					

Como elemento común se destaca en los documentos analizados, que los controles de seguridad se definen de manera general, sin entrar en detalles de soluciones tecnológicas para su implementación o ambientes de operación específicos. En todas las propuestas se establecen una amplia cantidad de controles, generalmente clasificados en dominios según la función que desempeñan en la seguridad del sistema. Aunque existe diversidad de criterios en cuanto a la cantidad de controles que proponen y su clasificación, usualmente permiten identificar áreas o dominios claves en los cuales se deben ejecutar determinados controles y el objetivo que persiguen.

En el caso de CIS la cantidad de controles se reduce considerablemente, pues solamente se consideran los 20 controles catalogados como los más críticos en un sistema de seguridad informática teniendo en cuenta los ataques que se producen con mayor frecuencia, aunque la cantidad de subcontroles totales sí resultan significativos. Como se observa, la cifra de controles propuestos por el NIST es muy superior, debido fundamentalmente a que comprende requisitos de seguridad mucho más estrictos, que responden al cumplimiento de leyes y regulaciones específicas de Estados Unidos, como la Ley FISMA10 y los estándares FIPS 19911 y FIPS 20012. Aunque los controles definidos por el CIS y el NIST no tienen en cuenta las características de la CN, los autores de esta investigación consideran que pueden ser también aplicables a un CD Virtualizado y a una NP.

La norma ISO/IEC 27017:2015 abarca tanto la provisión como el uso de los servicios de nube, modificando la guía de implementación de los controles definidos en la ISO/IEC 27002:2013, fundamentalmente los relacionados con el control de accesos, el cumplimiento, y la seguridad de las operaciones y las comunicaciones. Se observa que la mayoría de los cambios se concentran en el dominio de control de accesos, especialmente con respecto al registro y eliminación de los usuarios, el aprovisionamiento del acceso de los usuarios, la gestión de derechos de acceso privilegiado y la restricción del acceso a la información. Además, esta norma incorpora siete controles, distribuidos en los dominios: organización de la seguridad de la información, gestión de activos, control de accesos, seguridad de las operaciones, y seguridad de las comunicaciones. Estos nuevos controles se describen a continuación:

- El acuerdo sobre las responsabilidades compartidas o divididas entre el cliente y el Proveedor de Servicio de Nube (CSP, *Cloud Service Provider*), en torno a los roles de seguridad de la información asociados con los servicios en la nube, debe ser claramente establecido, registrado y comunicado.
- Se debe establecer cómo los activos son retornados o eliminados de la nube cuando el acuerdo entre el cliente y el proveedor ha terminado.
- El proveedor debe proteger y separar el entorno virtual del cliente de otros clientes y de partes externas.

[10] *Federal Information Security Management Act*. Ley federal establecida en Estados Unidos en el 2002 para la gestión de la seguridad de la información.
[11] *Federal Information Processing Standard*. Estándar para la Categorización de Seguridad de la Información Federal y los Sistemas de Información.
[12] *Federal Information Processing Standard*. Requerimientos Mínimos de Seguridad para la Información Federal y Sistemas de Información.

- El cliente y el proveedor deben asegurarse de que las Máquinas Virtuales (MV) estén configuradas y endurecidas[13] para satisfacer las necesidades de la organización.
- El cliente será responsable de definir, documentar y supervisar las operaciones y los procedimientos administrativos asociados con el entorno de la nube, y el proveedor debe compartir la documentación sobre operaciones y procedimientos críticos cuando los clientes así lo requieran.
- El proveedor debe garantizar capacidades que permitan al cliente monitorear la actividad dentro de un entorno de CN.
- Se deben hacer configuraciones consistentes para que el entorno de red virtual esté alineado con la política de seguridad de la información de las redes físicas.

El concepto de responsabilidad compartida es muy utilizado en las nubes públicas e híbridas, por ejemplo, los CSP Amazon Web Services (AWS) y Microsoft dividen la responsabilidad de la gestión de la seguridad, dejando al proveedor la seguridad de la infraestructura física y de virtualización, mientras que los clientes son los encargados de la seguridad de los Sistemas Operativos (SO) de las MV, las configuraciones, las credenciales de acceso, las aplicaciones y los datos [10,11]. Esto coincide con la delimitación de responsabilidades entre los diferentes roles del servicio de nube, que realiza la UIT-T en la Recomendación X.1642 en el caso de la categoría de Infraestructura como Servicio (IaaS, Infraestructure as a Service) [12].

Los autores de esta investigación consideran que para las NP el propietario de la nube es el máximo responsable de implementar los controles de seguridad a todos los niveles, que comprende desde la infraestructura física y virtual, hasta las aplicaciones y los datos que resulten críticos para el negocio, incluyendo los aspectos de seguridad relacionados con los recursos humanos. Sin embargo, los acuerdos sobre las responsabilidades compartidas entre el cliente y el proveedor, constituyen una herramienta muy útil inclusive en este modelo de despliegue, especialmente si se ofrece la categoría de IaaS a los usuarios. En este caso debe quedar establecido, mediante un acuerdo, que el proveedor o dueño de la nube será responsable de la seguridad de la capa de virtualización y gestión de nube hacia abajo, mientras que los usuarios responderán por la seguridad de los servicios que implementen sobre los recursos virtualizados y sus datos.

Por su parte la CSA aborda la seguridad como una necesidad que responde directamente a los objetivos del negocio y también separa las responsabilidades de los clientes y el CSP. Se observa en su propuesta un marcado enfoque en el cumplimiento de los estándares internacionales y algunos aspectos regulatorios regionales. Además, incorpora nuevos controles para garantizar la interoperabilidad de los CSP, como por ejemplo el uso de APIs (Application Programming Interfaces) abiertas y plataformas de virtualización reconocidas por la industria. También hace énfasis en la seguridad de los dispositivos móviles y BYOD14 que emplean los usuarios finales para conectarse a la nube e interactuar con los servicios.

En el caso de las regulaciones de Cuba, una de las principales limitaciones es que no se tienen en cuenta dominios de control claves como son la protección de los datos, la gestión de amenazas,

[13] Traducido del término en inglés *hardening*, concepto utilizado en seguridad informática para referirse a configuraciones optimizadas de sistemas operativos y aplicaciones, en función de fortalecer su seguridad y minimizar las vulnerabilidades.

[14] Bring Your Own Device (Trae Tu Propio Dispositivo) es una política empresarial consistente en que los empleados lleven sus propios dispositivos personales (portátiles, tabletas, móviles) a su lugar de trabajo para tener acceso a recursos de la empresa, tales como correos electrónicos, bases de datos y archivos en servidores.

vulnerabilidades y riesgos, el control automatizado de activos y la seguridad de la virtualización, esta última fundamental en los entornos de nube. Algo distintivo de la resolución cubana es que obliga a las entidades a implementar controles que permitan detectar y obstaculizar "la difusión de información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas; o que lesione la Seguridad Nacional" [9]. Esto implica la instalación de sistemas para el control de contenido, y la limitación de envío o recepción de mensajería masiva de correo electrónico, que sean configurables por frases y palabras claves.

SELECCIÓN DE LOS CONTROLES DE SEGURIDAD.

La selección e implementación de los controles se debe realizar después de identificar los requerimientos de seguridad, realizar la evaluación de los riesgos asociados a los activos de la organización, y decidir el tratamiento de los riesgos [13]. Partiendo de esto, los controles de seguridad deben garantizar que los riesgos identificados se reduzcan a un nivel aceptable, teniendo en cuenta lo siguiente:

- Los requisitos y restricciones de legislaciones y regulaciones nacionales e internacionales.
- Los objetivos organizacionales.
- Los requisitos y restricciones operacionales.
- El costo de la implementación y de la operación.
- Los objetivos para monitorear, evaluar y mejorar la eficiencia y efectividad de los controles de seguridad.
- La necesidad de balancear la inversión en la implementación y la operación de los controles, con respecto a la posible pérdida resultante de los incidentes de seguridad.

Debido a que la cantidad total de controles especificados en los documentos rectores analizados es muy elevada, se hace necesario identificar un conjunto razonable de controles a implementar, que proporcionen un nivel de seguridad apropiado a una NP o CD virtualizado, para organizaciones con limitaciones de financiamiento. Tomando como referencia la norma [5] de la ISO/IEC y los documentos de la CSA [7,14], se identificaron los principales dominios y controles de seguridad aplicables a las NP. De ese conjunto inicial de controles se decidió agrupar algunos de acuerdo al objetivo que persiguen o su modo de implementación. Por ejemplo, en los controles Planificación de la continuidad del negocio, y Política y procedimientos de mantenimiento y soporte, fueron incluidos las pruebas de los planes de continuidad del negocio, y la política y los procedimientos para garantizar la disponibilidad de las operaciones críticas del negocio.

Los criterios para la exclusión de algunos de los controles estuvieron basados fundamentalmente en que no pueden ser generalizados, o que resultan altamente complejos, en especial para entidades con limitaciones de financiamiento y/o recursos humanos. Por ejemplo, los Acuerdos de Confidencialidad no pueden ser aplicados en cualquier entidad, pues dependerá de la criticidad de sus sistemas y el tipo información que maneja su personal. Por otra parte, el cálculo de métricas para la respuesta a incidentes, como son el tiempo de detección, tiempo de mitigación, cantidad de incidentes, su clasificación por tipos, y costos de los incidentes, resulta complejo si no existe un sistema de gestión de incidentes que calcule estos valores de manera automática y genere las estadísticas. Otro control que no se consideró imprescindible es la separación de entornos de Producción y No-Producción, debido a que implica disponer de una mayor cantidad de recursos de HW. Sin embargo, si la organización tiene

las condiciones se recomienda crear un ambiente de desarrollo separado, con tecnologías similares a las desplegadas en la NP, para probar nuevos equipamientos y sistemas antes de ser instalados en el ambiente de producción.

Finalmente fueron seleccionados 41 controles, agrupados en 14 dominios, tal como se muestra en la Figura 1, los cuales comprenden no sólo medidas técnicas, sino también aspectos relacionados con el establecimiento de las políticas y los procedimientos. Los controles pueden ser preventivos, de detección o de recuperación, e incluyen además medidas administrativas, legales y educativas. Por su parte los procedimientos deben ser correctamente definidos y comprensibles a quienes corresponda su ejecución, lo que contribuye a la sistematicidad en la aplicación y al cumplimiento de las políticas de seguridad de la organización.

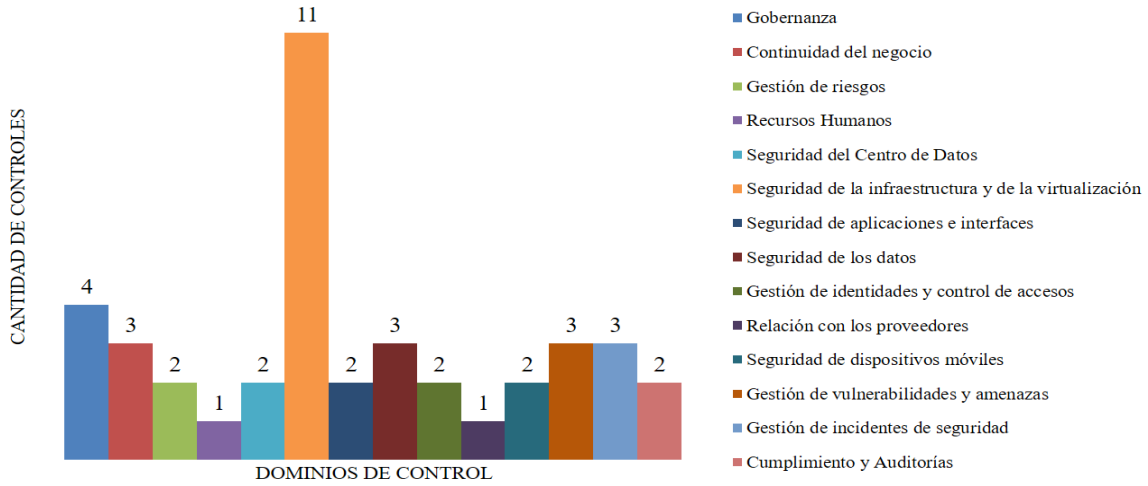

Figura 1: Controles de seguridad seleccionados para las NP agrupados por dominios.

Del total de controles de seguridad seleccionados para una NP o CD virtualizado, existe una cantidad considerable que resultan comunes a los CD tradicionales, como son los relacionados con la protección física, el respaldo energético, la gobernanza y la continuidad del negocio. Como se observa, la mayoría de los controles seleccionados corresponden al dominio de seguridad de la infraestructura y la virtualización. En esta categoría resulta relevante la seguridad y el endurecimiento de las MV y los hipervisores. Las nuevas MV que sean desplegadas bajo demanda en la nube deben crearse a partir de plantillas con configuraciones seguras y optimizadas, en función de las características del negocio. Las configuraciones de seguridad de las MV deben ser actualizadas teniendo en cuenta las nuevas vulnerabilidades y vectores de ataques que surjan, incluyendo las que permanecen inactivas. Además, la operación segura de las funciones administrativas del hipervisor y de la plataforma de gestión de nube es crítica. Su acceso debe estar restringido en base al principio de mínimos privilegios, y empleando comunicaciones cifradas mediante TLS/SSL (Transport Layer Security/Secure Sockets Layer) o SSH (Secure SHell). Es esencial el chequeo de la integridad de los componentes de SW del hipervisor y de la plataforma de gestión de nube, así como su correcta configuración y actualización.

Existen algunos controles importantes que deben ser adaptados a este escenario, pues su implementación en las NP y CD virtualizados difiere a los entornos TIC15 tradicionales. Tal es el caso de

15 Tecnologías de la Información y la Comunicación

la seguridad de la red y la detección de intrusiones, pues se requieren capacidades para detectar y controlar conexiones maliciosas o no autorizadas hacia la infraestructura de virtualización y la plataforma de gestión de nube, y además entre MV que corren sobre un mismo host. Esto implica la virtualización de sistemas IDS/IPS16 y la configuración de zonas de diferentes niveles de confianza mediante cortafuegos virtuales, o su implementación desde la propia plataforma de nube si ésta provee esas funcionalidades. Otro ejemplo es el proceso de la gestión de riesgos, en el cual se hace necesario asignarle valores máximos de activo a la infraestructura de virtualización y de gestión de la nube, y analizar las fuentes de riesgos particulares para este modelo de despliegue y la categoría de servicio que se implemente.

Adicionalmente, la Gestión de Accesos e Identidad (IAM, Identity and Access Management) es un control fundamental, pues garantiza que solamente las identidades autorizadas y autenticadas sean capaces de acceder a sus recursos y de la manera deseada. En las NP las medidas técnicas para restringir el acceso a los datos, aplicaciones y otros recursos (físicos y/o virtuales), deben estar en correspondencia con la separación de funciones y el principio de mínimos privilegios. La tendencia actual en las plataformas de nube es a soportar el modelo de Control de Acceso Basado en Atributos (ABAC, Attribute-Based Access Control) en lugar del modelo tradicional de Control de Acceso Basado en Roles (RBAC, Role-Based Access Control), en el que a menudo se emplea un único atributo (un rol definido). El modelo ABAC permite decisiones más detalladas y adaptadas al contexto mediante la incorporación de múltiples atributos como el rol, la ubicación, y el método de autenticación. La mayoría de los CSP, especialmente de IaaS, han implementado sistemas internos IAM, aunque es común que soporten Identidad Federada17. Entre los principales estándares utilizados en la CN para la gestión de identidad, autenticación y autorización se destacan SAML18, OpenID19 y OAuth20 [14].

Los autores de esta investigación recomiendan para las NP utilizar las funcionalidades IAM incorporadas en la plataforma de gestión de nube, disponiendo de un único punto de gestión de identidades y credenciales. Además se deben fortalecer los procesos de autenticación, por ejemplo mediante la Autenticación Multifactor (MFA, Multifactor Authentication)21, certificados digitales, establecer tiempos de expiración de las credenciales, niveles de complejidad para las contraseñas y prohibición de su reutilización.

[16] *Intrusion Detection/Prevention System*

[17] La gestión de Identidad Federada es el proceso de reafirmar una identidad a través de diferentes sistemas u organizaciones. Se ha vuelto popular con el crecimiento de las arquitecturas orientadas a servicios y es frecuente su empleo en los entornos de CN.

[18] Security Assertion Markup Language, desarrollado por OASIS. Actualmente en la versión 2.0. Es ampliamente soportado por herramientas empresariales y CSP. Mediante XML realiza la aserción entre el proveedor de identidad y el proveedor de servicio. El XML puede contener declaraciones de autenticación, de atributos y de decisiones de autorización.

[19] Es una estándar para autenticación federada que es ampliamente soportado por servicios web. Está basado sobre HTTP con URLs usadas para identificar el proveedor de identidad y la identidad de usuario. La versión actual es OpenID Connect 1.0 y es muy común en los servicios de consumidor.

[20] Es un estándar de IETF para la autorización que es utilizado fundamentalmente en servicios web. Es designado para trabajar sobre HTTP y actualmente está en la versión 2.0, que no es compatible con la 1.0. Es mayormente empleado para delegar la autorización y el control de accesos entre servicios.

[21] La implementación de MFA disminuye las amenazas relacionadas con el secuestro de cuentas, para ello pueden emplearse tokens de HW o SW, contraseñas fuera de banda como mensajes de texto enviados al móvil del usuario, y sensores biométricos.

Con respecto a los recursos humanos es necesario contar con un programa de preparación de los administradores del CD y especialistas de seguridad, que garantice el conocimiento y la actualización sobre las tecnologías de virtualización y de CN. Resulta útil la participación de los especialistas en foros de seguridad e intercambios con profesionales del sector, nacionales e internacionales. Además, es imprescindible la divulgación y concientización del resto del personal, así como de los usuarios, con respecto a las políticas de seguridad de la organización, sus responsabilidades y el uso seguro de los recursos, servicios y de la información.

PROPUESTA DE IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD EMPLEANDO SISTEMAS SLCA.

Constituye un reto para cualquier administrador de red o especialista de seguridad informática implementar la seguridad de una NP o CD virtualizado empleando únicamente sistemas de SLCA. La mayoría de las propuestas para asegurar este tipo de modelo de despliegue incluyen soluciones virtuales comerciales de Cortafuegos de Próxima Generación (NGFW)[22], *Network Packet Brokers* (NPB), Cortafuegos para Aplicaciones Web (WAF)[23], y herramientas para la microsegmentación. Estos por lo general con un alto nivel de integración con las plataformas de virtualización como VMware [15].

Entre los principales aspectos que deben ser analizados para la selección de una u otra solución de SLCA se encuentran: las funcionalidades y controles que cubre; su desempeño en infraestructuras virtualizadas; complejidad de despliegue, operación y mantenimiento; posibilidad de integración con otras herramientas; documentación pública disponible; requisitos de HW/SW para su implementación; facilidad de actualización; y desarrollo futuro, a mediano y largo plazo, por parte de la comunidad o de patrocinadores. No todos los controles pueden ser implementados a través de herramientas, pues algunos consisten en el establecimiento de políticas y procedimientos. En la Tabla 2 se muestra la propuesta de implementación de los controles, que comprende un grupo de herramientas de SLCA que pueden ser desplegadas para garantizar algunos de los controles seleccionados.

Tabla 2: Propuesta para la implementación de controles de seguridad en la NP.

Categoría	Controles	Referencias e Identificadores en Estándares y Regulaciones analizadas					Propuesta de implementación
		[5]	[6]	[7]	[8]	[9]	
Gobernanza	Políticas y procedimientos de seguridad	5.1.1 15.1.1	Todos XX-1	GRM-06	-	4; 6	Documentados dentro de un Plan de Seguridad Informática
	Responsabilidad de la dirección	7.2.1 18.2.2	PL-4 PS-6 PS-7 SA-9	GRM-03 GRM-05	-	7; 9; 16; 22; 38; 96	
	Programa de gestión de seguridad de la información	6.1.x	PM-1 PM-2 PM-3 PM-4 PM-8	GRM-04	-	4; 5	
	Política disciplinaria ante violaciones	7.2.3	PL-4 PS-1 PS-8	GRM-07	-	21; 99	Tanto el personal como los usuarios deberán firmar un documento aceptando las políticas de seguridad de la entidad, y la política

22 Next-Generation Firewall

23 Web Application Firewalls

							disciplinaria ante posibles violaciones.
Continuidad del Negocio	Planificación de la continuidad del negocio	17.1.1	CP-2	BCR-01	-	4; 86; 87	Documentado dentro de un Plan de Recuperación ante Contingencias.
	Documentación de los sistemas de información	parcialmente en 12.1.1	SA-5	BCR-04	-	parcialmente en 5	Documentados dentro de un Plan de Seguridad Informática
	Política y procedimientos de mantenimiento y soporte	parcialmente en 11.2.4 12.3.1	MA-2 MA-6 CP-6 CP-9	BCR-11	-	parcialmente en 38	
Gestión de Riesgos	Análisis / Evaluación de Riesgos	parcialmente en 12.6.1	RA-2 RA-3 RA-9	GRM-10	-	-	Puede emplearse la norma ISO/IEC 27005, el Marco de Gestión de Riesgos definido por el NIST u otros estándares y metodologías. Debe ser un proceso cíclico, cuyos resultados se incluirán en el Plan de Seguridad Informática. Se tendrán en cuenta, además de las fuentes de riesgo particulares de los entornos de nube, los riesgos medioambientales, los asociados con el acceso a los recursos corporativos desde dispositivos móviles, y las posibles interrupciones.
	Gestión / Tratamiento de Riesgos	11.1.4 11.2.1 11.2.2 6.2.1 15.1.1 15.2.2	PE-1 PE-9 PE-13 PE-14 PE-15 PE-18 PE-21 RA-3 CM-4 AC-17 AC-18 AC-19 SA-12	BCR-05 BCR-06 BCR-09 HRS-05 STA-01	-	parcialmente en 28; 29; 31; 32; 86; 87	
Recursos Humanos	Formación / Concientización	7.2.2	AT-1 AT-2 AT-3 AT-4 CP-3 IR-2 PM-14	HRS-05 HRS-09	17	12; 22	Moodle es una plataforma de gestión de cursos que puede ser utilizada en el entrenamiento del personal y los usuarios (https://moodle.org/) Distribución de boletines digitales mensuales vía correo electrónico sobre las principales amenazas. Si es posible publicar esta información en el sitio web interno de la organización.
Seguridad del Centro de Datos	Protección de servicios de suministro, condiciones medioambientales y respaldo energético	11.1.4 11.2.2 11.2.3 11.2.4	PE-1 PE-9 PE-10 PE-11 PE-12 PE-13 PE-14 PE-15 PE-21	BCR-03 BCR-08	-	parcialmente en 32	En el Plan de Seguridad Informática se definirán aquellas áreas seguras y el personal autorizado para el acceso. Se recomienda el empleo de las normas ISO/IEC 27002:2013 e ISO/IEC 27017:2015 para el establecimiento de los controles relacionados con la seguridad física del Centro de Datos.
	Perímetros de seguridad física. Autorización de acceso a las áreas seguras	11.1.1 11.1.2 11.1.6	PE-2 PE-3 PE-6 PE-8 PE-18	DCS-02 DCS-07 DCS-08 DCS-09	-	29; 30; 32; 33; 34; 35; 36	
Seguridad de la infraestructura	Inventario de activos	8.1.1 8.1.2	CM-8 PL-4	DCS-01	1; 2	parcialmente	OCS Inventory NG (https://www.ocsinventory-

y de la virtualización		8.1.3 8.1.4	PS-4 PS-5 PE-20			en 14	ng.org/en/) Open-AudIT (https://www.open-audit.org/) NMAP (https://nmap.org/)
	Gestión de configuraciones y control de cambios	12.1.2	CM-1 CM-2 CM-3 CM-5 CM-6 CM-9 CA-1 CA-6 CA-7	IVS-02 CCC-05	4; 11	-	Puppet, para gestión de configuraciones (http://puppetlabs.com/puppet/puppet-open-source/) OSSEC para el chequeo de integridad en ficheros de configuración (https://www.ossec.net/)
	Gestión de salvas y restauración	12.3.1	CP-6 CP-9 CP-10 AU-9	BCR-12	10	53; 54; 55; 56	Gestión de salvas propia de la plataforma de nube para las salvas de las instancias virtuales. Bacula, para las salvas a nivel de servicio (http://blog.bacula.org/). Tiene una versión de pago que permite la salva de la infraestructura virtualizada (https://www.baculasystems.com). Amanda Network Backup (http://www.amanda.org/)
	Seguridad de la red. Segmentación. Detección de intrusiones	9.1.2; 9.4.1; 9.5.1; 9.5.2; 13.1.X 18.1.4	SI-4 SC-7	IVS-01 IVS-06 IVS-09	6; 9; 11; 12	parcialmente en 58	pfSense (https://www.pfsense.org/) IPFire (https://www.ipfire.org/) Snort (https://www.snort.org/) Suricata (https://suricata-ids.org/) Kismet redes inalámbricas (https://www.kismetwireless.net/)
	Gestión de la capacidad	12.1.3	AU-4 AU-5 CP-2 SC-5 SC-6	IVS-04	-	-	Utilizar funcionalidad de la plataforma de gestión de nube
	Sincronización de relojes	12.4.4	AU-8	IVS-03	6	-	Configurar servidores de tiempo
	Monitoreo y registros de auditoría	12.4.1 12.4.2 12.4.3 16.1.2 16.1.7	AU-1 AU-2 AU-3 AU-4 AU-5 AU-6 AU-7 AU-9 AU-11 AU-12 AU-14 SI-4	IVS-01	6	parcialmente en 58	Una vez definidos los registros a colectar se puede implementar Elastic Stack (https://www.elastic.co/) o cualquier otra de las soluciones SLCA disponibles
	Instalaciones no autorizadas de	12.5.1 12.6.2	CM-1 CM-5	CCC-04	parcialm	parcialmente	Implementar Listas Blancas de Aplicaciones. Puede

	software		CM-7 CM-11 SI-7		ente en 2	en 10	resultar útil la guía del NIST SP 800-167 del 2015
	Seguridad y fortalecimiento de las imágenes de MV	9.5.2	CM-2	IVS-07	5	-	Creación de plantillas de referencia con configuraciones seguras y optimizadas, que deben ser actualizadas regularmente. Se recomienda el uso de las guías provistas por el Centro para la Seguridad de Internet (CIS Benchmarks, https://www.cisecurity.org/cis-benchmarks)
	Seguridad y fortalecimiento del hipervisor	-	-	IVS-11	-	-	Acceso cifrado y restringido a la administración del hipervisor en base al principio de mínimos privilegios. Garantizar su actualización. Implementar Buenas Prácticas del proveedor, y se recomienda estudiar las guías del NIST SP 800-125 y 800-125A.
	Protección de los datos en las migraciones	-	-	IVS-10	-	-	Cifrar la comunicación. Prohibir la migración hacia un *host* con niveles inferiores de seguridad.
Seguridad de Aplicaciones e Interfaces.	Seguridad de aplicaciones y datos intercambiados entre interfaces	9.4.1 9.4.2 12.6.1 13.2.1 13.2.2 14.2.1 14.2.3 14.2.7	AC-3 AC-4 AC-7 AC-8 AC-9 RA-3 RA-5 SA-3 SA-17 SC-2 SC-3 SC-8 SC-16 SC-23 CA-3	AIS-01 AIS-04	13; 18	-	Actualización de software. Cifrado de canales para la comunicación de los servicios.
	Adquisición y nuevos desarrollos	9.4.5 14.1.1 14.2.1 14.2.5 14.2.7 14.2.8 14.2.9	SA-1 SA-3 SA-4 SA-15 SA-17	CCC-01	-	parcialmente en 43	Debe crearse un programa de pruebas de aceptación para las nuevas adquisiciones. Los SW de desarrollo deben certificarse por las autoridades competentes. Por ejemplo, en Cuba CALISOFT.
Seguridad de los Datos y Gestión del Ciclo de Vida de la Información	Clasificación	8.2.1	RA-2 PM-29	DSI-01	parcialmente en 13	-	Clasificar los datos a partir de su sensibilidad. El tratamiento de la información clasificada deberá cumplir con las regulaciones existentes. Por ejemplo, en Cuba los documentos clasificados como Información Oficial deberán cumplir con el

							Decreto Ley 199/ 1999.
	Protección de datos sensibles. Criptografía	10.1.1 10.1.2 13.1.1 14.1.2 14.1.3 18.1.3 18.1.4	IA-7 SC-8 SC-12 SC-13 SC-16	EKM-03	13; 14	-	Protección mediante criptografía a los datos en reposo, en procesamiento y en tránsito. Se recomienda emplear métodos de encriptación tales como AES, RSA, y SHA-256 o superior; y establecer canales de comunicación seguros mediante TLS/SSL, IPsec o SSH. En el caso de Cuba la Resolución No. 2/2016 del Ministerio del Interior contiene el Reglamento sobre el funcionamiento de la Infraestructura de Llave Pública para la protección criptográfica de la Información Oficial.
	Eliminación Segura	8.3.2 11.2.7	MP-6	DSI-07	-	-	En caso de que la plataforma de nube o de la virtualización no provea opciones para el borrado seguro utilizar herramientas externas.
Gestión de identidades y control de accesos	Gestión de Identidad, Autenticación, Autorización, Control de Acceso	6.1.2 9.1.2 9.2.1 9.2.2 9.2.3 9.3.1 9.4.1 9.4.3	AC-2 AC-3 AC-5 AC- AC-24 IA-2 IA-4 IA-5 IA-8 PS-6 CM-5	IAM-05 IAM-09 IAM-12	4; 16	46; 48	IAM de la Plataforma de Nube para usuarios y grupos que acceden a las instancias virtuales MidPoint, sistema IAM opcional para el acceso a otros servicios que corran sobre la infraestructura de nube (https://evolveum.com/midpoint/)
	Gestión del aprovisionamiento	9.2.2	-	IAM-09	-	-	Funcionalidad de la Plataforma de Nube
Relación con los proveedores	Acuerdos con los proveedores	15.1.2 15.1.3	SA-4 SA-12	STA-05	-	-	Establecido mediante contrato legal entre ambas partes.
Seguridad de dispositivos móviles	Autorización del uso de dispositivos móviles para el acceso a servicios corporativos	6.2.1	AC-19	MOS-06	-	-	Revisión de los dispositivos móviles corporativos y los BYOD que podrán acceder a los servicios del negocio. Emisión por la dirección de la organización de un documento de autorización con las características técnicas de los equipos, que debe ser firmado por ambas partes.
	Inventario de dispositivos móviles conectados	-	-	MOS-09	1	-	OCS Inventory NG (https://www.ocsinventory-ng.org/en/)
Gestión de vulnerabilidades y amenazas	Control de software malicioso	12.2.1	SI-3	TVM-01	8	50	ClamAV (https://www.clamav.net/) Cuckoo Sandbox, plataforma para análisis automatizado de malware (https://cuckoosandbox.org/)

	Control de mensajería de correo electrónico no deseada	-	SI-8	-	7	79; 80; 81; 82	SpamAssassin (https://spamassassin.apache.org/) Rspamd (https://www.rspamd.com)
	Gestión de parches, vulnerabilidades y amenazas	parcialmente en 12.6.1	RA-5 SI-2	TVM-02	3	67	WSUS, para la actualización de SO Microsoft Windows. Repositorios actualizados para las distribuciones Linux. La actualización de la plataforma de gestión de nube y la infraestructura de virtualización, así como otros servicios de manera manual. OpenVas, para chequear la existencia de vulnerabilidades (www.openvas.org). OpenSCAP para escanear vulnerabilidades o configuraciones y evaluar cumplimiento mediante el estándar SCAP del NIST (https://www.open-scap.org/tools/). Loki, para el escaneo de Indicadores de Compromiso (https://github.com/Neo23x0/Loki).
Gestión de incidentes de seguridad	Contacto con las autoridades	6.1.3; 6.1.4	IR-6 SI-5 PM-15	SEF-01	19	91	Es obligatorio reportar de manera inmediata los incidentes o violaciones de seguridad informática a la instancia superior de la organización y a las autoridades competentes. En el caso de Cuba se debe reportar al CuCERT todos los incidentes de seguridad.
	Gestión de incidentes	16.1.1 16.1.2 16.1.4 16.1.5 16.1.7	IR-1 IR-2 IR-3 IR-4 IR-5 IR-7 IR-8	SEF-02	19	86; 87; 88; 89	OSSIM, SIEM de Alienvault que posee integración con herramientas de seguridad de código abierto como OCS Inventory, OpenVas, Nmap, Suricata, y OSSEC (https://www.alienvault.com/products/ossim). Security Onion, distribución que contiene múltiples herramientas para la detección y gestión de incidentes de seguridad como OSSEC, Snort, Suricata, Bro, Elastic Stack, FIR y otros (https://securityonion.net/).
	Comunicación de incidentes	16.1.2 16.1.3	IR-6 SI-5	SEF-03 STA-02	19	24; 89	Habilitar una cuenta de correo electrónico en la entidad para el reporte de incidentes de seguridad. Informar al personal y a los usuarios sobre los incidentes de seguridad mediante correo

							electrónico y el sitio web interno de la empresa.
Cumplimiento y Auditorías	Planificación de Auditorías	12.7.1	-	AAC-01	-	-	Se propone realizar auditorías internas como mínimo una vez al año.
	Auditorías Internas	18.2.1	CA-2 CA-7 RA-5	AAC-02	parcialmente 20	-	Pueden emplearse como referencia las normas ISO/IEC 27007:2017 e ISO/IEC TR 27008:2011, y las guías del NIST SP 800-115 y 800-53A Rev.5. Se recomienda la distribución Kali Linux para pruebas de penetración (https://www.kali.org/)

Se recomienda la integración a un sistema SIEM como el OSSIM, de la mayor cantidad de herramientas posibles, que permitan no sólo la colección de eventos y el monitorización, sino también la detección de diferentes vulnerabilidades y amenazas en tiempo real, así como su análisis y reporte. La principal desventaja de esta propuesta a criterio de los autores es la cantidad de recursos de procesamiento, memoria y almacenamiento que demanda la implementación de una solución SIEM basada en OSSIM. Debido a que esto puede suponer un obstáculo para aquellas entidades con presupuesto limitado, se plantea como alternativa el Security Onion. Específicamente se propone desplegar sensores OSSEC y Suricata (con las reglas abiertas de Emerging Threats), ElasticStack para el almacenamiento, análisis y visualización de los registros y eventos de seguridad, e instalar el OpenVAS como escaneador de vulnerabilidades y el sistema FIR para la gestión de los incidentes. Esta opción es relativamente menos compleja y su despliegue, configuración y optimización requiere menor tiempo. Los recursos necesarios estarán en dependencia de la cantidad de eventos a procesar, y si se pretende o no realizar la captura completa de los paquetes.

Los autores de esta investigación consideran que todas las soluciones de seguridad deben ser compatibles con el entorno virtual para obtener mayor flexibilidad, siendo la seguridad sin agente el modo más eficaz para proporcionar protección consistente y maximizar la densidad de MV sobre la infraestructura de HW. Por lo general en estas soluciones se implementa una “MV de Seguridad” en el servidor físico donde corren múltiples MV, en lugar de instalar un agente en cada MV, impactando menos en el rendimiento general del sistema. Sin embargo, las soluciones de SLCA disponibles emplean agentes para la monitorización, detección y control de las amenazas, por lo que deberán ser instaladas y evaluadas para comprobar su efectividad en la aplicación de los controles de seguridad, y otros aspectos importantes como son el impacto en el rendimiento y su escalabilidad.

CONCLUSIONES

Las organizaciones internacionales de estandarización y las regulaciones analizadas definen una amplia cantidad de controles de seguridad, aunque como se expuso solamente la ISO/IEC y la CSA tienen en cuenta las características específicas de los servicios de nube. Se considera que los controles que se proponen en este trabajo son un conjunto mínimo necesario para satisfacer los objetivos básicos de seguridad de una NP de cualquier organización, especialmente aquellas con limitaciones de financiamiento. Cada entidad podrá incorporar una mayor cantidad de controles, si así lo demandan sus

requerimientos, a medida que garanticen la implementación de los aquí presentados. Todos los controles que se establezcan inicialmente deberán ser evaluados de manera periódica, pudiendo ser sustituidos o mejorados cuando sea necesario.

Resulta vital la seguridad de la plataforma de virtualización utilizada en el despliegue de la nube, destacándose no solo las vulnerabilidades asociadas al hipervisor como elemento principal, sino también a los sistemas de gestión que conforman la plataforma de nube. Además, se recomienda implementar zonas con diferentes niveles de confianza, en especial si se tienen usuarios con distintos requerimientos de seguridad, que utilizan recursos virtuales que corren sobre el mismo conjunto de recursos físicos. Partiendo de ello se debe caracterizar bien el contexto, de esta forma se podrán establecer patrones de comportamiento habituales y detectar amenazas cuando exista una desviación de estos patrones, como pueden ser conexiones inusuales entre MV o *hosts*, transferencias de datos mayor que el valor medio, y tiempos de respuesta anómalos de determinados servicios.

En relación a las herramientas propuestas para la implementación de los controles se debe garantizar que no constituyan una afectación al rendimiento o a las capacidades de servicio soportadas, siendo recomendable evaluar su comportamiento en un ambiente de prueba, y su posible integración con la plataforma de gestión de la NP. La configuración de estas herramientas dependerá del contexto donde sean desplegadas, teniendo en cuenta las características de la infraestructura, los requerimientos de seguridad y las políticas de la organización.

REFERENCIAS

1. International Organization for Standardization. «ISO/IEC 27000:2016. Information security management systems. Overview and vocabulary». 2016 [citado 15 de noviembre de 2017]. Disponible en: https://www.iso.org/standard/66435.html

2. NIST. «Special Publication 800-53 Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations». NIST; 2015. Disponible en: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

3. ENISA. «Security aspects of virtualization». ENISA; 2017. Disponible en: https://www.enisa.europa.eu/publications/security-aspects-of-virtualization/at_download/fullReport

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

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

6. NIST. «Special Publication 800-53 Revision 5. Draft. Security and Privacy Controls for Information Systems and Organizations». NIST; 2017. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

7. Cloud Security Alliance. «Cloud Controls Matrix v3.0.1». Cloud Security Alliance; 2017. Disponible en: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

8. Center for Internet Security. «CIS Controls». [citado 30 de mayo de 2018]. Disponible en: https://www.cisecurity.org/controls/

9. «Resolución No. 127/2007. Reglamento de Seguridad Informática». Ministerio de Comunicaciones de Cuba; 2007. Disponible en: http://www.mincom.gob.cu/sites/default/files/marcoregulatorio/1346872659054_R%20127-07%20Reglamento%20de%20Seguridad%20Informatica.pdf

10. Amazon Web Services. Overview of Security Processes. 2016. Disponible en: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

11. Microsoft Corporation. Microsoft Cloud Security for Enterprise Architects. 2016. Disponible en: https://download.microsoft.com/download/6/D/F/6DFD7614-BBCF-4572-A871-E446B8CF5D79/MSFT_cloud_architecture_security.pdf
12. UIT-T. Recommendation X.1642. Directrices para la seguridad operativa de la computación en la nube. 2016. Disponible en: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12616
13. International Organization for Standardization. ISO/IEC 27000:2016 - Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary. 2016 [citado 15 de noviembre de 2017]. Disponible en: https://www.iso.org/standard/66435.html
14. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. 2017. Disponible en: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf
15. Sonny Sarai. Building the New Network Security Architecture for the Future. SANS Institute Reading Room; 2018. Disponible en: https://www.sans.org/reading-room/whitepapers/cloud/building-network-security-architecture-future-38255