risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 25/01/2019
Aceitação/Acceptance: 30/03/2019

Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones

Régner Sabillón[1], Jeimy J. Cano M.[2]

regners@athabascau.ca , jcano@uniandes.edu.co

[1] Universitat Oberta de Catalunya, Internet Interdisciplinary Institute (IN3), Parc Mediterrani de la Tecnologia (Edifici B3), Av. Carl Friedrich Gauss, 5, 08860 Castelldefels, Barcelona, España.

[2] Universidad de los Andes, Bogotá, Facultad de Derecho, Cra 1E No. 18ª-10, Bogotá, Colombia.

DOI: 10.17013/risti.32.33–48

Resumen: Este artículo presenta los resultados de un estudio de implementación y validación del Modelo de Auditoría de Ciberseguridad (CSAM), en un estudio de casos múltiples en una universidad canadiense. Se propone que el modelo se utilice para adelantar auditorías de ciberseguridad en cualquier organización o nación, y así evaluar la seguridad, su madurez y la preparación frente a la seguridad cibernética. De igual forma, detectar las necesidades para acrecentar la conciencia cibernética a nivel organizacional y personal. CSAM se ha probado, implementado y validado en tres escenarios de investigación (1) Auditoría de todos los dominios del modelo, (2) Auditoría de varios dominios y (3) una auditoría de un único dominio. El artículo concluye detallando información relevante para la toma de decisiones futuras con el fin de ajustar las limitaciones de ciberseguridad identificadas, mejorar sus dominios y controles, y de esta manera, implementar y probar de manera eficiente este modelo en cualquier organización o país.

Palabras-clave: Ciberseguridad; modelos de auditoría de ciberseguridad; auditorías en ciberseguridad; controles en ciberseguridad; aseguramiento en ciberseguridad.

Audits in Cybersecurity: A model of general application for companies and nations

Abstract: This article presents the results of an implementation and validation study of the Cybersecurity Audit Model (CSAM), in a multiple case study at a Canadian university. It is proposed that the model be used to advance cybersecurity audits in any organization or nation to assess security, its maturity, and preparedness for cybersecurity. Similarly, identify needs to increase cybersecurity awareness at the organizational and personal levels. CSAM has been tested, implemented and validated in three investigation scenarios (1) Audit of all model domains, (2) Audit of several domains and (3) an audit of a single domain. The article concludes by detailing relevant information for future decision making in order to adjust the identified cybersecurity limitations, improve their domains and controls, and thus efficiently implement and test this model in any organization or country.

***Keywords**:* Cybersecurity; cybersecurity audit models; cybersecurity audits; cybersecurity controls; cybersecurity assurance

1. Introducción

Las organizaciones tratan de proteger los activos cibernéticos e implementar medidas y programas de ciberseguridad, pero a pesar de este esfuerzo continuo, es inevitable que se presenten las violaciones de la ciberseguridad y se materialicen ataques cibernéticos.

Un estudio reciente (Hiscox, 2017) destaca que la incidencia de ataques cibernéticos es alta en compañías británicas, estadounidenses y alemanas de diferentes industrias y sectores, incluyendo tecnología, finanzas, servicios empresariales, manufactura, servicios profesionales, comercio minorista, construcción, transporte, alimentos y bebidas, salud, ocio, telecomunicaciones, bienes raíces, medios de comunicación, energía y productos farmacéuticos, desde pequeñas empresas hasta grandes corporaciones. El 57% de las empresas han experimentado al menos uno y el 42% de esas organizaciones se han ocupado de dos o más ataques cibernéticos en el último año. La mayoría de las empresas (62%) generalmente se recuperan de un incidente cibernético en menos de 24 horas; un cuarto (26%) generalmente toma menos de una hora para volver a los negocios, mientras que algunas compañías pasan dos días o más para recuperarse de un ataque cibernético. El análisis de brechas sugiere que invertir dinero o tener grandes presupuestos de seguridad cibernética no ayuda a las empresas a alcanzar el nivel de "Expertos en Internet". Por el contrario, un importante desembolso financiero no es la solución sino la implementación de otras medidas de estrategia y proceso, como la participación de la alta gerencia, la capacitación en concientización sobre la seguridad cibernética, el seguimiento sistemático y la documentación. Los costos de un ataque cibernético varían según las zonas geográficas, por ejemplo, con las empresas con más de 1.000 empleados, el impacto financiero costaría $ 53,131 en Alemania, $ 84,045 en el Reino Unido y $ 102,314 en los Estados Unidos (Hiscox, 2017).

Las auditorías de TI se están redefiniendo para incluir la ciberseguridad, sin que a la fecha existan pautas claras o consenso sobre qué áreas, subáreas, dominios o subdominios se incluirán en una auditoría de ciberseguridad. El modelo propuesto de auditoría de seguridad cibernética (CSAM), detallado en este artículo, ha sido diseñado para abordar las limitaciones y la inexistencia de controles de seguridad cibernética con el fin de materializar un programa de ciberseguridad o desarrollar auditorías de ciberseguridad específicas de dominio. Por tanto, un modelo extenso de auditoría de ciberseguridad puede apoyar la función de seguridad de la información y al mismo tiempo establecer un marco de trabajo para la concientización en seguridad de la información basada en los roles de la empresa.

Por tanto, se presentan los resultados de un estudio empírico que evaluó la implementación y validación del CSAM a través de una extensa auditoría de ciberseguridad. Este estudio fue motivado por la falta de directrices generales para llevar a cabo auditorías exhaustivas de ciberseguridad y las debilidades existentes de los programas disponibles a la fecha para impartir entrenamiento en concientización sobre la ciberseguridad.

Esta investigación se realizó con el propósito de dar respuesta a las siguientes interrogantes:

¿Cómo podemos evaluar y medir el nivel aseguramiento de la ciberseguridad, la madurez y la ciberpreparación en cualquier organización o Nación?

¿Por qué es necesario aumentar la ciberconciencia a nivel organizacional y personal?

2. Metodología

El objetivo de este estudio es investigar y proporcionar modelos integrales para los desafíos que puedan surgir al planificar y realizar auditorías de ciberseguridad, así como la implementación de la capacitación propia de la concientización sobre ciberseguridad. Entre los casos de estudio se consideran los más relevantes los estudios observacionales; los resultados de cualquier caso de estudio son limitados en generalización y aplicaciones más amplias (Edgard & Manz, 2017). Algunos autores prefieren diseñar sus casos de estudio utilizando la metodología de investigación de Yin (2009). Bartnes & Brede (2016) presentaron su investigación utilizando la recopilación de datos, el análisis de datos, las secciones de escenarios y contenido de casos. Meszaros & Buchalcevova (2016) diseñaron el Marco de Seguridad de Servicios Online (OSSF) y sus métodos de investigación se organizaron en un proceso con las siguientes actividades:

1. Identificación del problema y motivación.
2. Definición de objetivos para una solución.
3. Diseño y desarrollo.
4. Demostración
5. Evaluación
6. Comunicación

Luego de esta declaración, se ha diseñado, implementado y validado un estudio de casos múltiples basado en Yin (2018) de dos ejercicios: una auditoría de ciberseguridad y una capacitación de concientización sobre la ciberseguridad en una institución de educación superior canadiense. No es posible revelar más detalles de la organización objetivo por los acuerdos de confidencialidad establecidos. Se ha realizado este estudio de casos múltiples siguiendo la metodología de investigación propuesta por Yin (2018).

La motivación de este estudio tuvo como objetivo diseñar un modelo que incluyera un enfoque completo para planificar y realizar auditorías de ciberseguridad en cualquier organización con la capacidad para evaluar igualmente, las estrategias nacionales de ciberseguridad. Además, se identificó que era necesario lidiar con la falta de conocimiento para enfrentar los ataques y las amenazas cibernéticas, y como resultado, se diseñó un modelo organizacional de capacitación para la concientización sobre ciberseguridad que se puede implementar para fundar los elementos de cualquier programa de concientización sobre ciberseguridad.

3. Marco General de Gestión de Riesgos

Los modelos vigentes de ciberseguridad o de auditoría de ciberseguridad, responden por lo general a una gestión de riesgos conocidos. Las organizaciones basadas en sus

experiencias previas, resultados de ejercicios anteriores y revisiones de terceros, establecen un marco general de riesgos que terminan articulando en las ya conocidas matrices de riesgo-control, las cuales son revisadas y validadas en última instancia por los ejecutivos de las empresas (Cano, 2018).

En este contexto, las prácticas comunes de riesgo, generalmente articuladas desde el ISO 31000 e ISO 27005, establecen una serie pasos que buscan explorar de forma eficiente la manera como la organización se puede enfrentar a aquellas amenazas y actividades no deseadas previamente establecidas en el entorno (Díaz & Muñoz, 2018), dejando posiblemente fuera del radar aquellas que pueden afectarla gravemente por lo incierto de su manifestación.

De acuerdo con lo anterior, se hace necesario introducir un marco de trabajo de riesgos que actualice las prácticas actuales de su gestión, con el fin de ir más allá de los riesgos conocidos, y establecer un escenario extendido de revisión y análisis que dé cuenta tanto de las posibilidades como de las probabilidades. La ventana de AREM (Cano, 2014) es un marco de trabajo estratégico y táctico que no solo incluye los riesgos conocidos, sino que desarrolla aquellos que son propios del sector de la empresa que hace el ejercicio (riesgos focales), los latentes y los emergentes. Este instrumento, que ha sido probado en grandes empresas de energía como en el sector financiero, así como en la identificación y gestión de los riesgos de la infraestructura crítica de un país, permite a los auditores de ciberseguridad, movilizar sus reflexiones más allá del cuadrante de riesgos conocidos, para motivar conversaciones con las empresas para ver escenarios ampliados de amenazas, las cuales pueden no ser visibles desde el uso tradicional de los estándares.

Basado en lo anterior, la aplicación del Modelo de Auditoría de Ciberseguridad (CSAM), fundado en la gestión de riesgos usando la ventana de AREM, permite a los auditores mantener una sensibilidad concreta del entorno, que habilita una vista sistémica de los riesgos, para explorar en profundidad los diferentes dominios del modelo mencionado y buscar alternativas de aseguramiento que aumentan la confiabilidad de las prácticas de ciberseguridad de las empresas evaluadas.

4. El Modelo de Auditoría de CiberSeguridad (CSAM)

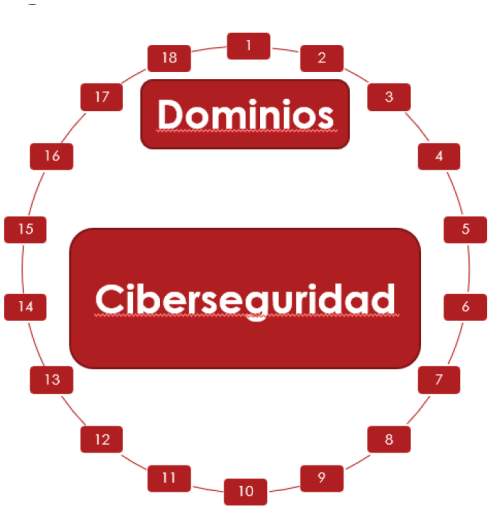
El Modelo de Auditoría de Ciberseguridad (CSAM) es un modelo innovador y exhaustivo que incluye la evaluación óptima de la ciberseguridad en cualquier organización y puede verificar pautas específicas para las naciones que planean implementar una estrategia nacional de seguridad cibernética o desean evaluar la efectividad de su Estrategia o Política Nacional de Ciberseguridad ya en vigor. El CSAM se puede implementar para llevar a cabo auditorías internas o externas de ciberseguridad, este modelo se puede usar para realizar auditorías de ciberseguridad individuales o puede ser parte de cualquier programa de auditoría corporativa para mejorar los controles de ciberseguridad. Cualquier equipo de auditoría tiene las opciones de realizar una auditoría completa para todos los dominios de ciberseguridad o simplemente seleccionando dominios específicos para auditar ciertas áreas que necesiten verificación de control y fortalecimiento. El CSAM tiene 18 dominios; el dominio 1 es específico para las Naciones y los dominios 2-18 se pueden implementar

en cualquier organización. La organización puede ser cualquier empresa pequeña, mediana o grande, el modelo también es aplicable a cualquier organización sin fines de lucro.

El objetivo de este trabajo es introducir un modelo de auditoría de ciberseguridad que incluya todas las áreas funcionales, a fin de asegurar una evaluación efectiva de ciberseguridad, su madurez y preparación cibernética en cualquier organización o Nación que esté auditando su Estrategia Nacional de Ciberseguridad. Esta propuesta se concibió como un modelo de auditoría de ciberseguridad integrado para evaluar y medir el nivel de madurez de la ciberseguridad y la preparación cibernética en cualquier tipo de organización, sin importar en qué industria o sector esté posicionada la organización. Muchos marcos de seguridad cibernética están orientados principalmente hacia una industria específica como el "PCI DSS" para la seguridad de las tarjetas de crédito, el "NERC CIP Cyber Security" para el sistema de energía eléctrica o el "Marco de seguridad cibernética del NIST" para proteger la infraestructura crítica nacional.

Sin embargo, los marcos existentes no proporcionan una vista unificada para la planificación y la realización de auditorías de ciberseguridad. La necesidad de alinear los marcos de seguridad cibernética específicos se debe a los requisitos regulatorios propios de las industrias, con el fin de cumplir con las auditorías internas o externas, y así satisfacer los propósitos comerciales y los requisitos del cliente o simplemente mejorar la estrategia de ciberseguridad de la empresa.

El Modelo de Auditoría de Ciberseguridad (CSAM) contiene información general, recursos, 18 dominios, 26 subdominios, 87 listas de verificación, 169 controles, 429 subcontroles, 80 evaluación de pautas y un cuadro de evaluación que se muestra en la Figura 1.



Dominios	Dominios
1- Naciones	10- Inteligencia de Amenazas
2- Gobernanza y Estrategia	11- Gestión de Incidentes
3- Marco Legal y Conformidad	12- Análisis Forense Digital
4- Activos Cibernéticos	13- Educación de Concientización
5- Riesgos Cibernéticos	14- Ciberseguros
6- Marcos y Regulaciones	15- Defensa Cibernética Activa
7- Arquitectura y Redes	16- Tecnologías Evolutivas
8- Información, Sistemas y Aplicaciones	17- Recuperación ante Desastres
9- Identificación de Vulnerabilidades	18- Gestión de Recursos Humanos

Figura 1 – Modelo de Auditoría de Ciberseguridad (CSAM)

4.1. Información General

Esta sección presenta la estructura del modelo, la metodología de trabajo y las posibles opciones de implementación.

4.2. Recursos

Este componente proporciona enlaces a recursos adicionales para ayudar a comprender los temas de ciberseguridad:

Ciberseguridad: Centro de Recursos de Seguridad Informática del Instituto Nacional de Estándares y Tecnología (NIST), prácticas de ciberseguridad de la Autoridad Reguladora de la Industria Financiera (FINRA) y ciberseguridad de la Seguridad Nacional (USA Homeland Security).

Estrategia nacional de ciberseguridad: Estrategia de ciberseguridad de la Organización del Tratado del Atlántico Norte (OTAN), estrategia de ciberseguridad de la Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA) y análisis comparativo de la Organización para la Cooperación y el Desarrollo Económico (OCDE) de las estrategias nacionales de ciberseguridad.

Gobernanza: Junta de Gobernanza de Ciberseguridad en PricewaterhouseCoopers y ciberseguridad de MITRE Corporation.

Activos cibernéticos: activos cibernéticos críticos de NERC (North American Electric Reliability Corporation).

Marcos: Marcos comunes de ciberseguridad de Foresite, el marco del Equipo de Preparación para Emergencias Informáticas de los EE.UU. (US-CERT) y el de ISACA (Information Systems Audit and Control Association) implementando el marco de ciberseguridad del NIST.

Arquitectura: Guía de arquitectos del TCG (Trusted Computer Group) y la arquitectura de seguridad de TI del Departamento de Energía de EE. UU.

Gestión de vulnerabilidades: Evaluación de vulnerabilidad SANS, evaluación y gestión de la seguridad nacional.

Inteligencia de amenazas cibernéticas: SANS (SysAdmin, Audit, Network and Security Institute): ¿Quién usa la inteligencia de amenazas cibernéticas y cómo?

Respuesta a incidentes: Preguntas frecuentes sobre el Equipo de respuesta a incidentes de seguridad informática (CSIRT – Computer Security Incident Response Team).

Análisis forense digital: Libros blancos de análisis forense SANS.

Conocimiento: NCSA (National Cyber Security Alliance) - Manténgase seguro online y PCI DSS (Payment Card Industry Data Security Standard): Mejores prácticas para implementar el programa de conocimiento de seguridad.

Defensa cibernética: SANS- La escala móvil de la ciberseguridad.

Recuperación ante desastres: FEI (Financial Executives International) Canadá - Ciberseguridad y continuidad de negocios.

Personal: Kaspersky - Los 10 mejores consejos para educar a los empleados sobre la ciberseguridad.

4.3. Dominios

El CSAM contiene 18 dominios. El dominio 1 ha sido diseñado exclusivamente para Naciones y los dominios 2-18 son aplicables a cualquier organización.

4.4. Subdominios

Todos los dominios tienen al menos un subdominio, pero en ciertos casos pueden existir varios subdominios por dominio.

Los subdominios son Ciberespacio, Gobernanza, Estrategia, Legal y Regulatorio, Gestión de Activos Cibernéticos, Riesgos Cibernéticos, Marcos y Regulaciones, Arquitectura, Redes, Información, Sistemas, Aplicaciones, Gestión de Vulnerabilidad, Inteligencia de Amenazas, Administración de Incidentes, Forensia Digital, Programa de Cibereducación Seguro Cibernético, Defensa Cibernética Activa, Tecnologías en Evolución, Recuperación de desastres, Contratación, Recursos Humanos, Habilidades, Capacitación y Despidos/ Renuncias.

4.5. Controles

Cada dominio tiene subdominios que tienen asignado un número de referencia. Los controles se identifican mediante números de cláusula y una lista de verificación asignada. Para verificar la evaluación de control, el control de ciberseguridad está definido o es inexistente.

4.6. Listas de Verificación

Cada lista de verificación está vinculada a un dominio específico y al subdominio subordinado. La lista de verificación verifica la validez de los subcontroles de ciberseguridad alineados con una cláusula de control. Los auditores de ciberseguridad tienen la opción de recopilar evidencia para verificar el cumplimiento del control secundario.

4.7. Evaluación de Directrices

La evaluación de la guía solo se aplica al dominio de las Naciones. Las directrices se evalúan para determinar la cultura de ciberseguridad, la Estrategia Nacional de Ciberseguridad (ENC), las operaciones cibernéticas, las infraestructuras críticas, la inteligencia cibernética, la guerra cibernética, la ciberdelincuencia y la diplomacia cibernética.

4.8. Cuadro de Evaluación

La evaluación de control, directriz y subcontrol se calcula después de que se haya completado la auditoría. La evaluación consiste en asignar puntajes y calificaciones para cada control, directriz y control secundario.

Se calcula la clasificación final de la madurez de la ciberseguridad del dominio de las Naciones utilizando los siguientes criterios. La puntuación se puede asignar a un nivel de madurez específico:

Inmaduro (I): 0-30

La Nación no tiene planes para administrar su ciberespacio. Una Estrategia o Política Nacional de Ciberseguridad (ENC) es inexistente.

En desarrollo (D): 31-70

La Nación está empezando a centrarse en la ciberseguridad nacional. Si las tecnologías están en su lugar, la Nación debe centrarse en áreas clave para proteger el ciberespacio.

Maduro (M): 71-90

Mientras que la Nación tiene un ambiente maduro. Se requieren mejoras en áreas claves que se han identificado con debilidades.

Avanzado (A): 91-100

La Nación se ha destacado en la ciberseguridad nacional y en las prácticas del ciberespacio. Siempre hay espacio para mejorar. La Nación podría convertirse en un líder internacional y ayudar a otros Estados en temas de ciberseguridad y ciberespacio.

Y para los dominios 2-18, calculamos la calificación final de madurez de la ciberseguridad de cualquier organización utilizando los siguientes criterios:

La puntuación se puede asignar a un nivel de madurez específico:

Inmaduro (I): 0-30

La organización no tiene planes para gestionar su ciberseguridad. Los controles para las áreas críticas de ciberseguridad son inexistentes o muy débiles. La organización no ha implementado un programa integral de ciberseguridad.

En desarrollo (D): 31-70

La organización está empezando a centrarse en asuntos de ciberseguridad. Si las tecnologías están en su lugar, la organización debe centrarse en áreas clave para proteger los activos cibernéticos. La atención debe estar enfocada hacia el personal, procesos, controles y regulaciones.

Maduro (M): 71-90

Mientras que la organización tiene un ambiente maduro. Se requieren mejoras en las áreas claves que se han identificado con debilidades.

Avanzado (A): 91-100

La organización ha destacado en la implementación de las mejores prácticas de ciberseguridad. Siempre existen posibilidades para la mejora continua. Se debe mantener la documentación correspondiente actualizada y revisar continuamente los procesos de ciberseguridad a través de auditorías y basado en el marco general de riesgos latentes y emergentes.

5. Resultados

El CSAM se implementó y validó utilizando tres escenarios diferentes en la institución de educación superior canadiense. Para implementar y validar el CSAM, también diseñamos el CATRAM que se implementó simultáneamente junto con el CSAM. Nuestras preguntas de investigación se abordaron adecuadamente mediante la creación y validación de dos modelos de ciberseguridad en las áreas de auditoría y concientización. La organización objetivo consideró los tres escenarios como realistas para su evaluación, capacitación de sensibilización, aseguramiento y auditoría de ciberseguridad. Se concluye que los dos modelos de ciberseguridad son funcionales y útiles según se observa en los resultados de la validación (Tabla 1). Por lo tanto, los modelos de ciberseguridad son susceptibles de implementar y probar en cualquier organización. Blokdyk (2018) utiliza un enfoque similar para presentar los resultados del cuadro de mando de ciberseguridad. Esta autoevaluación de la ciberseguridad presenta el cuadro de mando ilustrado en un gráfico de radar, que destaca un sistema de puntaje de siete criterios que incluye el reconocimiento, la definición, la medición, el análisis, la mejora, el control y el mantenimiento de los asuntos de ciberseguridad con un enfoque en la gestión de riesgos.

No.	Ciberdominios	Resultados
2	Gobernanza y Estrategia	35%
3	Marco Legal y Conformidad	90%
4	Activos Cibernéticos	30%
5	Riesgos Cibernéticos	60%
6	Marcos y Regulaciones	30%
7	Arquitectura y Redes	67%
8	Información, Sistemas y Aplicaciones	55%
9	Identificacion de Vulnerabilidades	30%
10	Inteligencia de Amenazas	60%
11	Gestión de Incidentes	10%
12	Análisis Forense Digital	30%
13	Educación de Concientización	60%
14	Ciberseguros	90%
15	Defensa Cibernética Activa	5%
16	Tecnologias Evolutivas	100%
17	Recuperacion ante Desastres	30%
18	Gestión de Recursos Humanos	77%
Nivel de Madurez en Ciberseguridad		**51%**

Tabla 1 – Nivel de Madurez basado en múltiples ciberdominios

El siguiente resumen presenta oportunidades al mejorar y fortalecer las medidas de seguridad cibernética en nuestra organización objetivo.

Dominios de ciberseguridad que necesitan atención inmediata basada en la auditoría CSAM:

Marcos y regulaciones (30%): La organización necesita seleccionar un marco o componentes de seguridad específicos de varios marcos de seguridad de la información para implementar los marcos deseados. Se debe seleccionar un marco de ciberseguridad para garantizar la protección de las áreas funcionales, la gestión de riesgos, los controles de seguridad y la auditoría.

Identificación de vulnerabilidades (30%): La organización necesita implementar un plan de evaluación de vulnerabilidad. Se requiere un plan para implementar el escaneo continuo, las pruebas de penetración, la evaluación de vulnerabilidades, las medidas de corrección de vulnerabilidades y buscar la alineación con el panorama actual de amenazas cibernéticas y los riesgos existentes.

Gestión de incidentes (10%): La organización necesita saber cómo afrontar los ataques cibernéticos. Un plan de acción es urgente. La organización necesita un plan de acción para implementar la gestión de respuesta a incidentes, establecer niveles de escalamiento y comunicación, educación y concientización de incidentes, una política corporativa de gestión de incidentes y definir el procedimiento para todas las fases de respuesta a incidentes cibernéticos.

Análisis forense digital (30%): Ya sea para contratar consultores externos o capacitar a su personal de TI, la organización debe tener un plan que debe formar parte de la gestión de incidentes cibernéticos de su organización. La organización no está familiarizada con los procedimientos de investigación digital, los procedimientos de cadena de custodia y las investigaciones de descubrimiento electrónico.

Defensa cibernética activa (5%): La organización necesita implementar controles de ciberseguridad para todas las áreas de negocios. La organización no ha implementado controles críticos para aplicar la defensa cibernética activa, detectar y analizar ataques cibernéticos, mitigar daños cibernéticos y contramedidas externas fuera de sus redes.

Recuperación ante desastres (30%): La organización necesita agregar e integrar la ciberseguridad para su Recuperación ante desastres (DR) y su Plan de continuidad comercial (BCP). Si bien se han tomado algunas medidas para la recuperación general de desastres, la ciberseguridad no se ha considerado en ningún caso de interrupciones, ni en las evaluaciones para los escenarios posteriores a la reanudación.

Gobernanza y estrategia (35%): La organización debe definir su estrategia de seguridad cibernética e implementar un programa de ciberseguridad organizacional que esté alineado con la estrategia, misión, visión, metas y objetivos de la institución.

Dominios de ciberseguridad que necesitan mejoras en función de la auditoría CSAM:

Riesgos cibernéticos (60%): La organización necesita diseñar, implementar y revisar regularmente un plan de administración de riesgos cibernéticos. Se requiere una clara clasificación de los activos de información. Además, se necesita una política de gestión de riesgos cibernéticos bien definida, que incluya metas y objetivos junto con una matriz para aceptar, mitigar o transferir riesgos cibernéticos.

Activos cibernéticos (60%): Los activos cibernéticos deben identificarse y protegerse. Se requieren auditorías de inventario para identificar los activos cibernéticos y se requieren propietarios dentro de la organización.

Arquitectura y redes (67%): La organización necesita implementar controles adicionales para fortalecer la arquitectura y la seguridad de las redes. Las áreas que necesitan mejoras son defensa en profundidad, seguridad física, seguridad para productos y servicios de terceros, marcos de arquitectura, encriptación, pruebas de penetración, gestión de cuentas de usuarios y gestión del rendimiento.

Información, sistemas y aplicaciones (55%): La organización necesita implementar controles adicionales para reforzar la seguridad de la información, los sistemas y las aplicaciones. Las áreas que necesitan mejoras son la gestión de proyectos, la gestión de cambios, la gestión de registros, los controles y evaluaciones de auditoría, la gestión web, la planificación de recursos empresariales (ERP), la seguridad de las aplicaciones, los controles de salida de aplicaciones, los controles de seguimiento de auditoría de aplicaciones y los controles de correo electrónico.

Inteligencia de amenazas (60%): La organización necesita comenzar a recopilar y procesar información sobre posibles amenazas cibernéticas, vulnerabilidades cibernéticas y posibles ataques cibernéticos que pueden afectar sus operaciones. La organización debe dedicar recursos y equipos para mejorar la recopilación de inteligencia sobre amenazas y para implementar las políticas de respuesta requeridas.

Educación de concientización (60%): La organización necesita implementar un programa completo de concientización y capacitación sobre ciberseguridad para todas las partes interesadas. El entrenamiento parcial de concientización es ineficaz. Si bien CATRAM se implementó por completo como punto de partida para desarrollar el programa corporativo de concientización y capacitación sobre ciberseguridad, se

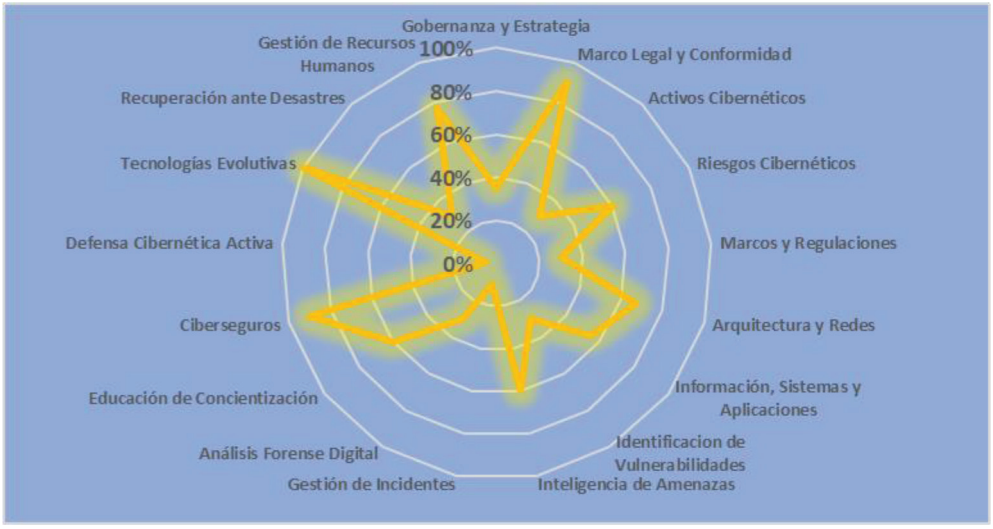


Figura 2 – Gráfico de Radar del estudio CSAM

recomienda particularmente realizar revisiones anuales para enfrentar las nuevas amenazas cibernéticas.

El estudio del caso demostró que el alcance de la investigación se logró según lo establecido. La evidencia para esta conclusión se presenta en la Figura 2.

6. Conclusiones

El objetivo principal de esta investigación fue diseñar y validar el Modelo de Auditoría de Ciberseguridad (CSAM) para enfrentar los desafíos al realizar auditorías de ciberseguridad integrales. El modelo de ciberseguridad que incluye todos sus componentes, fue validado satisfactoriamente por un caso de estudio realizado en una institución de educación superior canadiense.

El CSAM no es exclusivo para una industria, sector u organización. Por el contrario, el modelo se puede utilizar para planificar, realizar y verificar auditorías de ciberseguridad en cualquier organización o país. El CSAM ha sido diseñado para realizar auditorías de ciberseguridad parciales o completas para un dominio específico, varios dominios o para la auditoría integral de todos los dominios.

Los resultados de este estudio muestran que las auditorías de ciberseguridad realizadas por dominios pueden ser muy efectivas para evaluar los controles y las respuestas a las amenazas cibernéticas.

La limitación de nuestro estudio es que el modelo se validó en una sola organización, las limitaciones de tiempo, la falta de interés por los temas y la falta de compromiso fueron algunos de los desafíos que tuvimos que superar por parte de los participantes e investigadores. Por lo tanto, actualmente estamos realizando una segunda validación en una universidad canadiense diferente y más grande, que permita comprobar con nuevos datos de investigación científica el diseño y la efectividad del CSAM.

Los resultados de la investigación tienen implicaciones para nuestra organización objetivo, pero al mismo tiempo, implicaciones para futuras investigaciones en las que se pueda revisar y ampliar los modelos de ciberseguridad propuestos, integrando dentro de la dinámica de aplicación de éstos, la ventana de AREM, como soporte estratégico de riesgos y amenazas emergentes para los auditores de ciberseguridad (Cano, 2017).

Referencias

Bartnes, M., Brede, N., & Heegaard, P.E. (2016). The future of information security incident management training: A case study of electrical power companies. *Computers & Security*. (61). 32–45. doi: 10.1016/j.cose.2016.05.004

Bartnes, M., & Moe, N.B. (2017). Challenges in IT security preparedness exercises: A case study. *Computers and Security*. (67). 280–290. doi: 10.1016/j.cose.2016.11.017

Blokdyk, G. (2018). *Cyber Security Risk Management: Complete Self-Assessment Guide*. *Brisbane*: Emereo Publishing.

Cano, J. (2014). La ventana de AREM. Una herramienta estratégica y táctica para visualizar la incertidumbre. *Actas de la XIII Reunión Española de Criptología y Seguridad de la Información*. Alicante, España. Septiembre 2 al 5. Recuperado de: http://web.ua.es/es/recsi2014/documentos/papers/la-ventana-de-arem-una-herramienta-estrategica-y-tactica-para-visualizar-la-incertidumbre.pdf

Cano, J. (2017). The AREM Window: A Strategy to Anticipate Risk and Threats to Enterprise Cyber Security. *ISACA Journal*. 5 (2017).

Cano, J. (2018). Repensando los fundamentos de la gestión de riesgos. Una propuesta conceptual desde la incertidumbre y la complejidad. *Revista Ibérica de Tecnología y Sistemas de la Información*. (E15). Abril. 76–87.

Center for Audit Quality – CAQ (2017). The CPA's Role in Addressing Cybersecurity Risk: How the Auditing Profession Promotes Cybersecurity Resilience. Washington, DC: CAQ-AICPA.

CERT Division (2017). CSIRT Frequently Asked Questions. Pittsburgh, PA: Carnegie Mellon University. Recuperado de https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm

Deloitte University Press (2016). Deloitte-NASCIO Cybersecurity Study- State goverments at risk: Turning strategy and awareness into progress. Deloitte Development LLC. Recuperado de: https://www.nascio.org/Portals/0/Publications/Documents/2016/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf

Díaz, O. & Muñoz, M. (2018). Implementación de un enfoque DevSecOps + Risk Management en un Centro de Datos de una organización Mexicana. RISTI - *Revista Ibérica de Tecnología y Sistemas de la Información*. (26) 43–53. Doi: 10.17013/risti.26.

Donaldson, S., Siegel, S., Williams, C., & Aslam, C. (2015). *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats (pp* 201-204). New York, USA.: Apress.

Edgar, T., & Manz, D. (2017). *Research Methods for Cyber Security (pp* 143-144). Cambridge: Elsevier.

Financial Executives International (2014). Financial Executives, Cyber Security & Business Continuity. Toronto, Ontario: Canadian Executives Research Foundation. Recuperado de: https://www.feicanada.org/enews/file/CFERF%20studies/2013-2014/IBM%20Cyber%20Security%20final3%202014.pdf

Financial Industry Regulatory Authority (2015). Report on Cybersecurity Practices: February (pp 1- 46). Recuperado de: https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

Hathaway, M., Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2015). Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index. Arlington: Potomac Institute for Policy Studies. Recuperado de: http://www.potomacinstitute.org/images/CRIndex2.0.pdf

Hiscox (2017). Hiscox Cyber Readiness Report. London: Forrester Consulting. Recuperado de: https://www.hiscox.com/documents/brokers/cyber-readiness-report.pdf

ISACA (2014). Implementing the NIST Cybersecurity Framework. Rolling Meadows: ISACA.

ISACA (2016). IS Audit/Assurance Program – Cybersecurity: Based on the NIST Cybersecurity Framework. Rolling Meadows: ISACA.

Kaspersky Lab (2015). Top 10 Tips for Educating Employees about Cybersecurity. AO Kaspersky Lab. Recuperado de: http://go.kaspersky.com/rs/kaspersky1/images/Top_10_Tips_For_Educating_Employees_About_Cybersecurity_eBook.pdf

Khan, M. (2016). Managing Data Protection and Cybersecurity-Audit's Role. *ISACA Journal*, 1(2016).

Leidos (2017). Core Security Framework Assessment. Recuperado de: https://cyber.leidos.com/services/core-security-framework-assessment

Leidos (2017). Cyber Defense Maturity Scorecard: Defining Cybersecurity Maturity Across Key Domains. Recuperado de: https://www.leidos.com/sites/g/files/zoouby166/files/2018-08/CDMEScorecard_Digital.pdf

Messier, R. (2016). *Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems*. New York: Apress. ISBN 978-1-4842-1856-3.

Meszaros, J., & Buchalcevova, A. (2016). Introducing OSSF: A framework for online service cybersecurity risk management. *Computers & Security*. (65). 300–313.

Ministry of Economic Affairs and Communication (2017). 2014-2017 Estonia Cybersecurity Strategy. Iráklio, Greece : ENISA. Recuperado de https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf

National Association of State Chief Information Officers (NASCIO), Grant Thornton & CompTIA (2017). The 2017 State CIO Survey. Recuperado de: https://www.comptia.org/communities/resources/2017-state-cio-survey

National Cyber Security Alliance (2017). Stay Safe Online. NCS. Recuperado de: https://staysafeonline.org/ncsam/

National Institute of Standards and Technology (2017). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1, January.

National Institute of Standards and Technology (2017). NIST Special Publications SP. Recuperado de: http://csrc.nist.gov/publications/PubsSPs.html

North Atlantic Treaty Organization. Cooperative Cyber Defence Centre of Excellence (2015). Cyber Security Strategy Documents. August. Recuperado de: https://ccdcoe.org/strategies-policies.html

North American Electric Reliability Corporation (2010). Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets. NERC. Recuperado de: www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf

Organisation for Economic Co-Operation and Development (2012). Cybersecurity Policy Making at a Turning Point. OECD. Recuperado de: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Payment Card Industry. Security Standards Council (2014). Best Practices for implementing a Security Awareness Program. PCI DSS, October. Recuperado de: https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Pricewaterhouse Coopers (2016). PwC's Board Cybersecurity Governance Framework. PwC. Recuperado de: https://www.pwc.com/ca/en/consulting/publications/20160310-pwc-reinforcing-your-organizations-cybersecurity-governance.pdf

Protiviti (2017). A Global Look at IT Audit Best Practices: Assessing the International Leaders in an Annual ISACA/Protiviti Survey. Protiviti Inc.

Protiviti (2017). Board Perspectives: Risk Oversight. Protiviti Inc. Recuperado de https://www.protiviti.com/US-en/taxonomy/term/3566

Ross, S. (2015). Cybersecurity for a "Simple" Auditor. *ISACA Journal*. 6(2018).

Sabillon, R. (2018). A Practical Model to Perform Comprehensive Cybersecurity Audits. Enfoque UTE, *9*(1), 127 - 137. doi: https://doi.org/10.29019/enfoqueute.v9n1.214

Sabillon, R., Serra, J., Cavaller, V., & Cano, J. (2017). A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). In: *Proceedings of the 2nd International Conference on Information Systems and Computer Science* (INCISCOS). IEEE Xplore Digital Library, 253-259. doi: https://doi.org/10.1109/INCISCOS.2017.20

Sabillon, R., Serra, J., Cavaller, V., & Cano, J. (2018). An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). In: *Proceedings of the 1st International Conference on Information Systems and Management Science* (ISMS). University of Malta, Misida, Malta.

SANS Institute (2017). SANS Forensics Whitepapers. SANS Institute. Recuperado de https://digital-forensics.sans.org/community/whitepapers

United States Computer Emergency Readiness Team (2017). Cybersecurity Framework. US-CERT. Recuperado de https://www.us-cert.gov/ccubedvp/cybersecurity-framework

U.S. Department of Homeland Security (2016). Cybersecurity. September. Recuperado de https://www.dhs.gov/topic/cybersecurity

Yin, R.K. (2009). *Case Study Research: Design and Methods*. 4th ed. Los Angeles, CA: Sage Publications.

Yin, R.K. (2014). *Case Study Research: Design and Methods*. 5th ed. Thousand Oaks, CA: Sage Publications.

Yin, R.K. (2018). *Case Study Research and Applications*. 6th ed. Thousand Oaks, CA: Sage Publications.